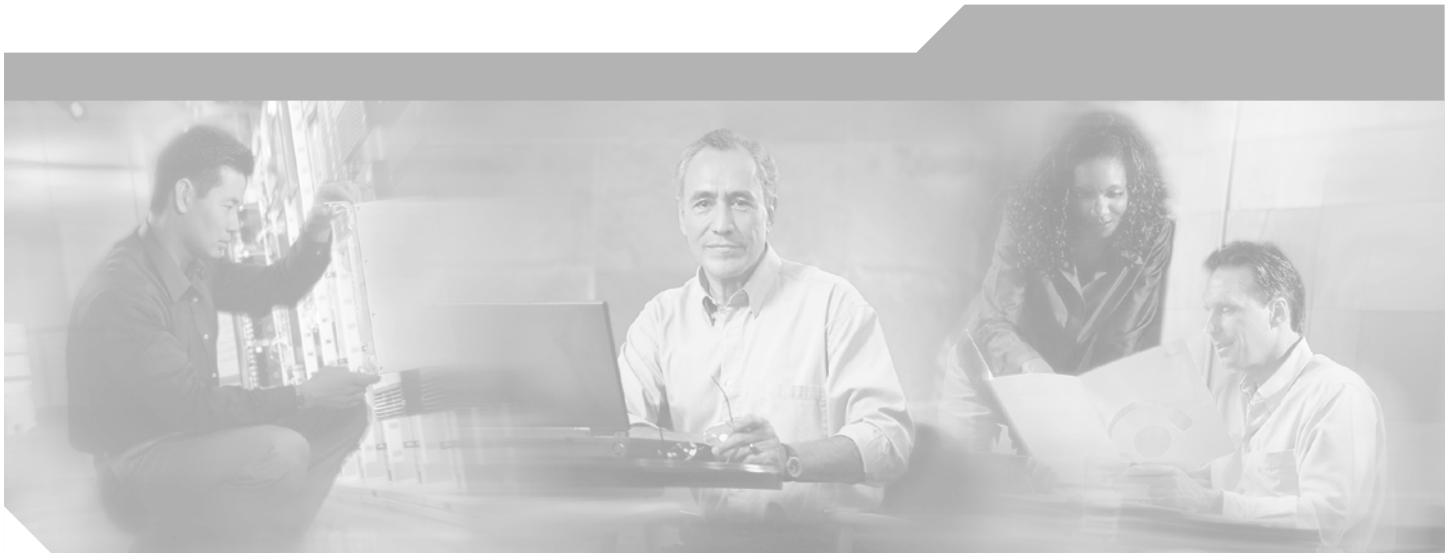


Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-4211-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide
Copyright © 2005 Cisco Systems, Inc.
All rights reserved.

CONTENTS

Preface xi

- Audience xii
- Purpose xii
- Organization xii
- Conventions xiii
- Related Publications xv
- Obtaining Documentation xv
  - Cisco.com xv
  - Documentation DVD xv
  - Ordering Documentation xvi
  - Documentation Feedback xvi
- Cisco Product Security Overview xvi
  - Reporting Security Problems in Cisco Products xvii
- Obtaining Technical Assistance xvii
  - Cisco Technical Support Website xvii
  - Submitting a Service Request xviii
  - Definitions of Service Request Severity xviii
- Obtaining Additional Publications and Information xix

CHAPTER 1

Product Overview 1-1

- Introduction to the Client Adapters 1-2
  - Terminology 1-2
- Hardware Components 1-3
  - Radio 1-3
  - Radio Antenna 1-3
  - LEDs 1-3
- Software Components 1-4
  - Driver 1-4
  - Client Utilities 1-4
- Network Configurations Using Client Adapters 1-5
  - Ad Hoc Wireless LAN 1-5
  - Wireless Infrastructure with Workstations Accessing a Wired LAN 1-6

CHAPTER 2 **Preparing for Installation** 2-1

Safety information 2-2
FCC Safety Compliance Statement 2-2
Safety Guidelines 2-2
Warnings 2-2
Unpacking the Client Adapter 2-3
Package Contents 2-3
System Requirements 2-4
Site Requirements 2-5
For Infrastructure Devices 2-5
For Client Devices 2-5

CHAPTER 3 **Installing the Client Adapter** 3-1

Inserting a Client Adapter 3-2
Inserting a PC-Cardbus Card 3-2
Inserting a PCI Card 3-3
Changing the Bracket 3-3
Inserting the Card 3-4
Assembling the Antenna 3-5
Mounting the Antenna 3-6
Installing the Client Adapter Software 3-9
Installing a Microsoft Hot Fix for Group Policy Delay 3-20

CHAPTER 4 **Using the Profile Manager** 4-1

Overview of Profile Manager 4-2
Opening Profile Manager 4-2
Creating a New Profile 4-4
Including a Profile in Auto Profile Selection 4-7
Selecting the Active Profile 4-9
Modifying a Profile 4-10
Editing a Profile 4-10
Deleting a Profile 4-10
Importing and Exporting Profiles 4-10
Importing a Profile 4-11
Exporting a Profile 4-11

CHAPTER 5 **Configuring the Client Adapter** 5-1

Overview 5-2

Setting General Parameters 5-3

Setting Advanced Parameters 5-6

Setting Security Parameters 5-13

Overview of Security Features 5-14

Static WEP Keys 5-15

EAP (with Dynamic WEP Keys) 5-15

WPA and WPA2 5-18

CCKM Fast Secure Roaming 5-18

Reporting Access Points that Fail LEAP Authentication 5-19

Additional WEP Key Security Features 5-20

Synchronizing Security Features 5-20

Enabling Static WEP 5-24

Enabling WPA/WPA2 Passphrase 5-26

Enabling LEAP 5-27

Enabling EAP-FAST 5-31

Deleting a Manually Provisioned PAC File 5-38

Enabling EAP-TLS or PEAP 5-39

Enabling EAP-TLS 5-40

Enabling PEAP (EAP-GTC) 5-42

Enabling PEAP (EAP-MSCHAP V2) 5-46

Enabling PEAP (EAP-MSCHAP V2) Machine Authentication with Machine Credentials 5-49

Disabling Static WEP, WPA/WPA2 Passphrase, or EAP 5-51

Enabling Wi-Fi Multimedia 5-51

Enabling the QoS Packet Scheduler on Windows 2000 5-51

Enabling the QoS Packet Scheduler on Windows XP 5-54

Setting Roaming Parameters in the Windows Control Panel 5-55

CHAPTER 6 **Using EAP Authentication** 6-1

Overview 6-2

Using LEAP or EAP-FAST 6-2

Using LEAP or EAP-FAST with the Windows Username and Password 6-3

After Profile Activation or Card Insertion 6-3

After a Reboot or Logon 6-4

After Your EAP-FAST Password Expires 6-4

Using LEAP or EAP-FAST with an Automatically Prompted Login 6-5
After Profile Activation or Card Insertion 6-5
After a Reboot or Logon 6-6
After Your EAP-FAST Password Expires 6-7
Using LEAP or EAP-FAST with a Manually Prompted Login 6-8
After Profile Activation 6-8
After a Reboot, Logon, or Card Insertion 6-9
After Your EAP-FAST Password Expires 6-11
Using LEAP or EAP-FAST with a Saved Username and Password 6-12
After Profile Activation or Card Insertion 6-12
After a Reboot or Logon 6-12
After Your EAP-FAST Password Expires 6-13
Using EAP-TLS 6-13
Using PEAP (EAP-GTC) 6-14
Windows NT or 2000 Domain Databases or LDAP Databases Only 6-14
OTP Databases Only 6-14
Using PEAP (EAP-MSCHAP V2) 6-15
Restarting the Authentication Process 6-15

CHAPTER 7 **Viewing Status and Statistics** 7-1
Overview of ADU Status and Statistics Tools 7-2
Setting Parameters that Affect ADU Status and Statistics Tools 7-2
Viewing the Current Status of Your Client Adapter 7-4
Viewing Statistics for Your Client Adapter 7-12

CHAPTER 8 **Using the Aironet System Tray Utility (ASTU)** 8-1
Overview of ASTU 8-2
The ASTU Icon 8-2
Tool Tip Window 8-3
Pop-Up Menu 8-5
Help 8-5
Exit 8-6
Open Aironet Desktop Utility 8-6
Troubleshooting 8-6
Preferences 8-6
Enable/Disable Radio 8-7
Manual Login 8-8
Reauthenticate 8-8

Select Profile 8-8
Show Connection Status 8-9

CHAPTER 9 **Routine Procedures 9-1**

Removing a Client Adapter 9-2
Removing a PC-Cardbus Card 9-2
Removing a PCI Card 9-2
Client Adapter Software Procedures 9-3
Upgrading the Client Adapter Software 9-3
Uninstalling the Client Adapter Software 9-6
ADU Procedures 9-7
Opening ADU 9-7
Exiting ADU 9-7
Finding the Version of ADU 9-8
Viewing Client Adapter Information 9-8
Accessing Online Help 9-9
ASTU Procedures 9-9
Enabling or Disabling Your Client Adapter's Radio 9-9

CHAPTER 10 **Troubleshooting 10-1**

Accessing the Latest Troubleshooting Information 10-2
Interpreting the Indicator LEDs 10-2
Troubleshooting the Client Adapter 10-3
Using the Troubleshooting Utility 10-3
Diagnosing Your Client Adapter's Operation 10-3
Saving the Detailed Report to a Text File 10-7
Disabling the Microsoft Wireless Configuration Manager (Windows XP Only) 10-8
Disabling the Microsoft 802.1X Supplicant (Windows 2000 Only) 10-8
Client Adapter Recognition Problems 10-8
Resolving Resource Conflicts 10-9
Resolving Resource Conflicts in Windows 2000 10-9
Resolving Resource Conflicts in Windows XP 10-10
Problems Associating to an Access Point 10-10
Problems Connecting to the Network 10-11
Prioritizing Network Connections 10-11
Parameters Missing from Profile Management Windows 10-11
Windows Wireless Network Connection Icon Shows Unavailable Connection (Windows XP Only) 10-11
Error Messages 10-12

APPENDIX A **Technical Specifications** A-1

APPENDIX B **Translated Safety Warnings** B-1

Explosive Device Proximity Warning B-2

Antenna Installation Warning B-3

Warning for Laptop Users B-4

APPENDIX C **Declarations of Conformity and Regulatory Information** C-1

Manufacturer's Federal Communication Commission Declaration of Conformity Statement C-2

Department of Communications – Canada C-3

Canadian Compliance Statement C-3

European Community, Switzerland, Norway, Iceland, and Liechtenstein C-3

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC C-3

Declaration of Conformity Statement C-5

Cisco Aironet CB21AG Wireless LAN Client Adapter C-5

Cisco Aironet PI21AG Wireless LAN Client Adapter C-6

Declaration of Conformity for RF Exposure C-7

Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan C-7

Japanese Translation C-7

English Translation C-7

Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan C-8

2.4- and 5-GHz Client Adapters C-8

Chinese Translation C-8

English Translation C-8

5-GHz Client Adapters C-9

Chinese Translation C-9

English Translation C-9

APPENDIX D **Channels, Power Levels, and Antenna Gains** D-1

Channels D-2

IEEE 802.11a D-2

IEEE 802.11b/g D-3

Maximum Power Levels and Antenna Gains D-4

IEEE 802.11a D-4

IEEE 802.11b D-4

IEEE 802.11g D-5

APPENDIX E **Configuring the Client Adapter through the Windows XP Operating System** E-1

Overview E-2

Overview of Security Features E-2

Static WEP Keys E-2

EAP (with Dynamic WEP Keys) E-3

WPA E-4

Configuring the Client Adapter E-5

Enabling EAP-TLS Authentication E-10

Enabling PEAP Authentication E-13

Enabling PEAP (EAP-MSCHAP V2) E-14

Enabling PEAP (EAP-GTC) E-16

Associating to an Access Point Using Windows XP E-18

Viewing the Current Status of Your Client Adapter E-18

APPENDIX F **Performing a Site Survey** F-1

Overview F-2

Guidelines F-2

Additional Information F-2

Opening the Site Survey Utility F-3

Selecting the Client Adapter F-3

Using the Associated AP Status Tab F-4

Specifying Display Units F-4

Viewing the Access Point's Status F-5

Using the AP Scan List Tab F-8

Viewing the AP Scan List F-9

Pausing the AP Scan List F-11

Viewing AP Details F-12

Generating an AP Scan Log File F-14

Finding the Version of the Site Survey Utility F-15

Accessing Online Help F-15

Exiting the Site Survey Utility F-15

Uninstalling the Site Survey Utility F-15

GLOSSARY

INDEX

Preface

The preface provides an overview of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary.

The following topics are covered in this section:

- Audience, page xii
- Purpose, page xii
- Organization, page xii
- Conventions, page xiii
- Related Publications, page xv
- Obtaining Documentation, page xv
- Cisco Product Security Overview, page xvi
- Obtaining Technical Assistance, page xvii
- Obtaining Additional Publications and Information, page xix

Audience

This publication is for the person responsible for installing, configuring, and maintaining a Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapter (CB21AG or PI21AG) on a computer running the Microsoft Windows 2000 or XP operating system. This person should be familiar with computing devices and with network terms and concepts.

Note Windows 2000 and XP are the only supported operating systems.

Purpose

This publication describes the Cisco Aironet CB21AG and PI21AG client adapters and explains how to install, configure, and troubleshoot them.

Caution This manual pertains specifically to Cisco Aironet CB21AG and PI21AG client adapters, whose software is incompatible with that of other Cisco Aironet client adapters. Refer to the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* if you are installing or using 340, 350, or CB20A cards.

Organization

This publication contains the following chapters:

- Chapter 1, "Product Overview," describes the client adapters and their hardware and software components and illustrates two common network configurations.
- Chapter 2, "Preparing for Installation," provides information that you need to know before installing a client adapter, such as safety information and system requirements.
- Chapter 3, "Installing the Client Adapter," provides instructions for installing the client adapter.
- Chapter 4, "Using the Profile Manager," explains how to use the Aironet Desktop Utility (ADU) profile manager feature to create and manage profiles for your client adapter.
- Chapter 5, "Configuring the Client Adapter," explains how to change the configuration parameters for a specific profile.
- Chapter 6, "Using EAP Authentication," explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is activated.
- Chapter 7, "Viewing Status and Statistics," explains how to use ADU to view the client adapter's status and its transmit and receive statistics.
- Chapter 8, "Using the Aironet System Tray Utility (ASTU)," explains how to use ASTU to view status information about your client adapter and perform basic tasks.
- Chapter 9, "Routine Procedures," provides procedures for common tasks related to the client adapters, such as uninstalling client adapter software and opening ADU.
- Chapter 10, "Troubleshooting," provides information for diagnosing and correcting common problems that may be encountered when installing or operating a client adapter.

- Appendix A, “Technical Specifications,” lists the physical, radio, power, and regulatory specifications for the client adapters.
- Appendix B, “Translated Safety Warnings,” provides translations of client adapter safety warnings in nine languages.
- Appendix C, “Declarations of Conformity and Regulatory Information,” provides declarations of conformity and regulatory information for the client adapters.
- Appendix D, “Channels, Power Levels, and Antenna Gains,” lists the IEEE 802.11a, b, and g channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.
- Appendix E, “Configuring the Client Adapter through the Windows XP Operating System,” explains how to configure and use your client adapter with the Microsoft Wireless Configuration Manager.
- Appendix F, “Performing a Site Survey” shows people who are responsible for conducting a site survey how they can use the site survey utility to determine the best placement for infrastructure devices within a wireless network.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands are in **boldface**.
- Variables are in *italics*.
- Configuration parameters are capitalized.
- Notes, cautions, and warnings use the following conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico’s en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

For more information about Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters for Windows, refer to the following publication:

- *Release Notes for Cisco Aironet 802.11a/b/g Client Adapters (CB21AG and PI21AG) Install Wizard*

For more information about related Cisco Aironet products, refer to the publications for your infrastructure device. You can find Cisco Aironet technical documentation at this URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Product Overview

This chapter describes the Cisco Aironet CB21AG and PI21AG client adapters and illustrates their role in a wireless network.

The following topics are covered in this chapter:

- Introduction to the Client Adapters, page 1-2
- Hardware Components, page 1-3
- Software Components, page 1-4
- Network Configurations Using Client Adapters, page 1-5

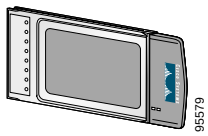
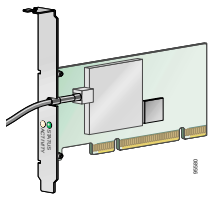
Introduction to the Client Adapters

The Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) are radio modules that provide wireless data communications among fixed, portable, and mobile devices within both wireless and wired network infrastructures. The client adapters are fully compatible when used in devices supporting “plug-and-play” (PnP) technology.

The primary function of the client adapters is to transfer data packets through the wireless infrastructure by communicating with other clients or with access points that are connected to a wired LAN. The adapters operate similarly to a standard network product except that radios rather than Ethernet cables make the connection to the wire. No special wireless networking functions are required, and all existing applications that operate over a network can operate using the adapters.

This document covers the two client adapters described in Table 1-1.

Table 1-1 Client Adapter Types

Client Adapter	Model Number	Description	Illustration
PC-Cardbus card	AIR-CB21AG	An IEEE 802.11a/b/g-compliant 2.4- and 5-GHz 54-Mbps client adapter card radio module with a Cardbus interface that can be inserted into any device equipped with a 32-bit Cardbus slot. Host devices can include laptops and notebook computers.	
PCI card	AIR-PI21AG	An IEEE 802.11a/b/g-compliant 2.4- and 5-GHz 54-Mbps client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot, such as a desktop personal computer.	

Terminology

The following terms are used throughout this document:

- **client adapter**—Refers to both types of adapters.
- **PC-Cardbus card** or **PCI card**—Refers to a specific adapter.
- **workstation** (or **station**)—Refers to a computing device with an installed client adapter.
- **infrastructure device**—Refers to a device that connects client adapters to a wired LAN, such as an access point, bridge, or base station. Throughout this document, *access point* is used to represent infrastructure devices in general.

Hardware Components

The client adapters have three major hardware components: a radio, a radio antenna, and two LEDs.

Radio

The client adapters contain a dual-band radio that is both IEEE 802.11a and 802.11b/g compliant. The radio uses both direct-sequence spread spectrum (DSSS) technology and orthogonal frequency division multiplexing (OFDM) technology for client applications in the 2.4-GHz Industrial Scientific Medical (ISM) frequency band and OFDM technology in the 5-GHz Unlicensed National Information Infrastructure (UNII) frequency bands. The client adapters operate with other IEEE 802.11a or 802.11b/g-compliant client devices in ad hoc mode or with Cisco Aironet access points and other IEEE 802.11a or 802.11b/g-compliant infrastructure devices in infrastructure mode.

Radio Antenna

The type of antenna used depends on your client adapter:

- PC-Cardbus cards have an integrated, permanently attached 0-dBi gain, dual-band 2.4/5-GHz diversity antenna. The benefit of the diversity antenna system is improved coverage. The system works by enabling the card to sample and switch between its two antenna ports in order to select the optimum port for receiving data packets. As a result, the card has a better chance of maintaining the radio frequency (RF) connection in areas of interference. The antenna is housed within the section of the card that hangs out of the Cardbus slot when the card is installed.
- PCI cards have a 1-dBi gain, dual-band 2.4/5-GHz antenna that is permanently attached by a 6.6-foot (2-meter) cable. A base is provided with the antenna to enable it to be mounted to a wall or to sit upright on a desk or other horizontal surface.

LEDs

The client adapters have two LEDs that glow or blink to indicate the status of the adapter or to convey error messages. Refer to Chapter 10 for an interpretation of the LED codes.

Software Components

The client adapters have two major software components: a driver and client utilities. These components are installed together by running a single executable Install Wizard file that is available from Cisco.com. This file can be run on Windows 2000 or XP and can be used only with CB21AG and PI21AG client adapters.

Note Chapter 3 provides instructions on using the Install Wizard to install these software components.

Driver

The driver provides an interface between a computer's operating system and the client adapter, thereby enabling the operating system and the applications it runs to communicate with the adapter. The driver must be installed before the adapter can be used.

Client Utilities

Two client utilities are available for use with the client adapters: Aironet Desktop Utility (ADU) and Aironet System Tray Utility (ASTU). These utilities are optional applications that interact with the client adapter's radio to adjust settings and display information.

ADU enables you to create configuration profiles for your client adapter and perform user-level diagnostics. Because ADU performs a variety of functions, it is documented by function throughout this manual.

ASTU, which is accessible from an icon in the Windows system tray, provides a small subset of the features available through ADU. Specifically, it enables you to view status information about your client adapter and perform basic tasks. Chapter 8 provides detailed information and instructions on using ASTU.

Note If your computer is running Windows XP, you can configure your client adapter through the Microsoft Wireless Configuration Manager (or another third-party tool) instead of through ADU. Refer to Appendix E for information. However, ADU is recommended for configuring the client adapter.

Network Configurations Using Client Adapters

Client adapters can be used in a variety of network configurations. In some configurations, access points provide connections to your network or act as repeaters to increase wireless communication range. The maximum communication range is based on how you configure your wireless network.

This section describes and illustrates the two most common network configurations:

- Ad hoc wireless local area network (LAN)
- Wireless infrastructure with workstations accessing a wired LAN

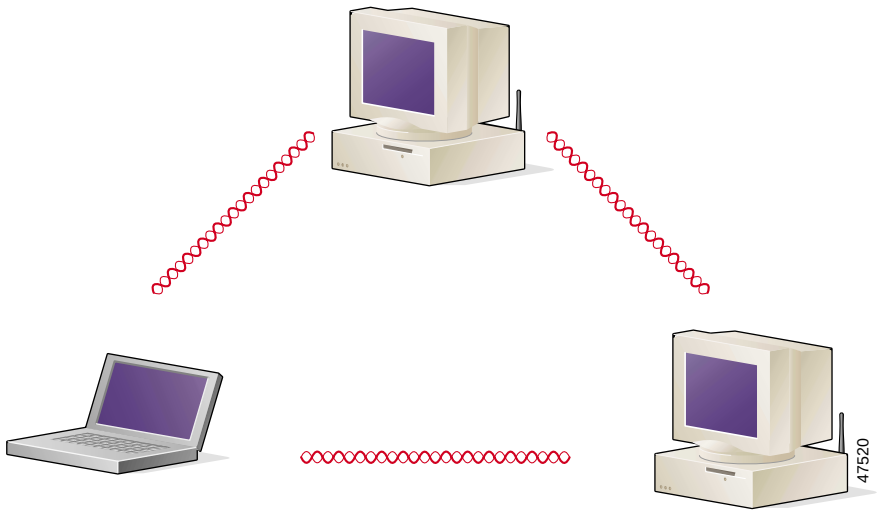
For examples of more complex network configurations involving client adapters and access points, refer to the documentation for your access point.

Note Refer to Chapter 5 for information on setting the client adapter's network type.

Ad Hoc Wireless LAN

An ad hoc (or *peer-to-peer*) wireless LAN (see Figure 1-1) is the simplest wireless LAN configuration. In a wireless LAN using an ad hoc network configuration, all devices equipped with a client adapter can be linked together and communicate directly with each other. The use of an infrastructure device, such as an access point, is not required.

Figure 1-1 Ad Hoc Wireless LAN

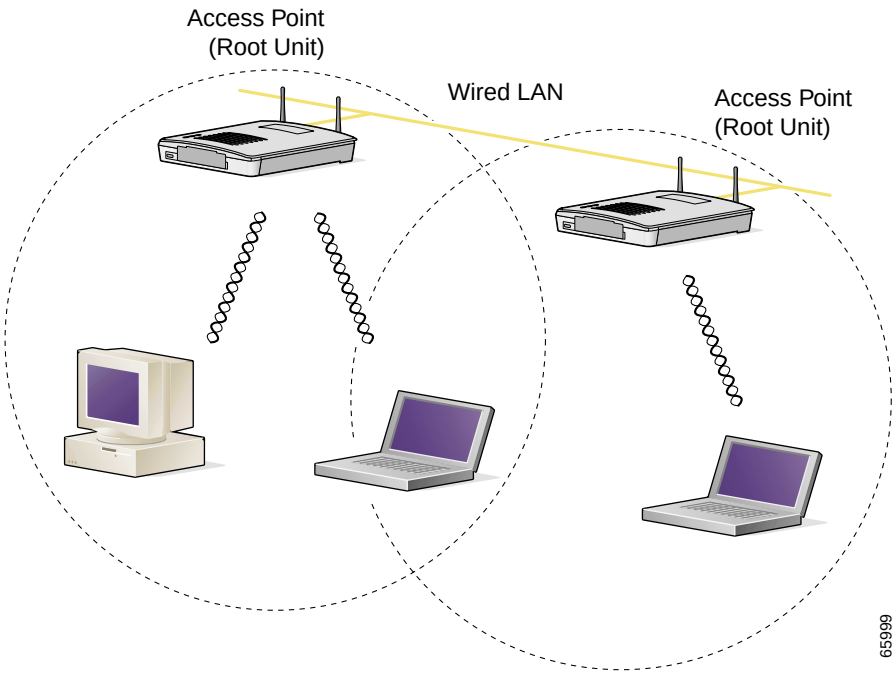


Wireless Infrastructure with Workstations Accessing a Wired LAN

A microcellular network can be created by placing two or more access points on a LAN. Figure 1-2 shows a microcellular network with workstations accessing a wired LAN through several access points.

This configuration is useful with portable or mobile stations because it enables them to be directly connected to the wired network even while moving from one microcell domain to another. This process is transparent, and the connection to the file server or host is maintained without disruption. The mobile station stays connected to an access point as long as it can. However, when the transfer of data packets needs to be retried or beacons are missed, the station automatically searches for and associates to another access point. This process is referred to as *seamless roaming*.

Figure 1-2 Wireless Infrastructure with Workstations Accessing a Wired LAN



Preparing for Installation

This chapter provides information that you need to know before installing a client adapter.

The following topics are covered in this chapter:

- Safety information, page 2-2
- Unpacking the Client Adapter, page 2-3
- System Requirements, page 2-4
- Site Requirements, page 2-5

Safety information

Follow the guidelines in this section to ensure proper operation and safe use of the client adapter.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication will result in user exposure substantially below the FCC recommended limits.

Safety Guidelines

- Do not touch or move the antenna while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Warnings

Observe the following warnings when operating the client adapter. The second warning pertains to the PI21AG client adapter, and the third warning pertains to the CB21AG client adapter.

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.**

Warning **This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PC Card slots that can provide at least 0.394 in (1 cm) separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.**

Translated versions of these safety warnings are provided in Appendix B.

Unpacking the Client Adapter

Follow these steps to unpack the client adapter:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in the "Package Contents" section below are included in the shipment. Check each item for damage.

Note If any item is damaged or missing, notify your authorized Cisco sales representative.

Package Contents

Each client adapter is shipped with the following items:

- 1-dBi gain antenna permanently attached by a 6.6-ft (2-m) cable, antenna base, low-profile bracket, two mounting screws, and two plastic wall anchors (PCI cards only)
- *Quick Start Guide: Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG)*
- Cisco Aironet 802.11a/b/g Wireless Adapters (CB21AG and PI21AG) CD

System Requirements

In addition to the items shipped with the client adapter, you also need the following items in order to install and use the adapter:

- One of the following computing devices running Windows 2000 or XP:
  - Laptop or notebook computer equipped with a 32-bit Cardbus slot
  - Desktop personal computer equipped with an empty PCI expansion slot

Note Cisco recommends a 300-MHz (or greater) processor.

- Service Pack 2 for Windows XP
- 20 MB of free hard disk space (minimum)
- 128 MB of RAM or greater (recommended)
- The appropriate tools for removing your computer's cover and expansion slot dust cover and for mounting the antenna base (for PCI cards)
- If your wireless network uses EAP-TLS or PEAP authentication, Certificate Authority (CA) and user certificates for EAP-TLS authentication or CA certificate for PEAP authentication
- If your wireless network uses PEAP (EAP-GTC) authentication with a One-Time Password (OTP) user database:
  - A hardware token device from OTP vendors or the Secure Computing SofToken program (version 2.1 or later)
  - Your hardware or software token password
- The following information from your system administrator:
  - The logical name for your workstation (also referred to as *client name*)
  - The protocols necessary to bind to the client adapter, such as TCP/IP
  - The case-sensitive service set identifier (SSID) for your RF network
  - If your network setup does not include a DHCP server, the IP address, subnet mask, and default gateway address of your computer
  - The wired equivalent privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security
  - The username and password for your network account
  - Protected access credentials (PAC) file if your wireless network uses EAP-FAST authentication with manual PAC provisioning

Site Requirements

This section discusses the site requirements for both infrastructure and client devices.

For Infrastructure Devices

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Therefore, before you install any wireless infrastructure devices (such as access points, bridges, and base stations, which connect your client adapters to a wired LAN), a site survey must be performed to determine the optimum placement of these devices to maximize range, coverage, and network performance. Appendix F, which is provided for people who are responsible for conducting a site survey, explains how the site survey utility can be used to determine the best placement for infrastructure devices within a wireless network.

Note Infrastructure devices are installed and initially configured prior to client devices.

For Client Devices

Because the client adapter is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

- Install the client adapter in an area where large steel structures such as shelving units, bookcases, and filing cabinets will not obstruct radio signals to and from the client adapter.
- Install the client adapter away from microwave ovens. Microwave ovens operate on the same frequency as the client adapter and can cause signal interference.

Installing the Client Adapter

This chapter provides instructions for installing the client adapter.

The following topics are covered in this chapter:

- Inserting a Client Adapter, page 3-2
- Installing the Client Adapter Software, page 3-9
- Installing a Microsoft Hot Fix for Group Policy Delay, page 3-20

Inserting a Client Adapter

This section provides instructions for inserting a PC-Cardbus card or PCI card into your computer.

Caution These procedures and the physical connections they describe apply generally to conventional Cardbus slots and PCI expansion slots. In cases of custom or nonconventional equipment, be alert to possible differences in Cardbus slot and PCI expansion slot configurations.

Inserting a PC-Cardbus Card

Step 1 Before you begin, examine the card. One end has a dual-row, 68-pin connector. The card is keyed so it can be inserted only one way into the Cardbus slot.

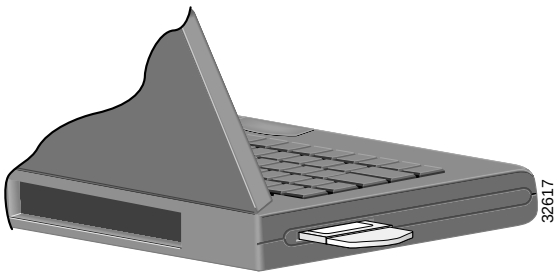
Note The Cardbus slot is on the left or right side of the computer, depending on the model.

Step 2 Turn on your computer and let the operating system boot up completely.

Step 3 Hold the card with the Cisco label facing up and insert it into the Cardbus slot, applying just enough pressure to make sure it is fully seated (see Figure 3-1). The green LED lights when the card is inserted properly.

Caution Do not force the card into your computer's Cardbus slot. Forcing it will damage both the card and the slot. If the card does not insert easily, remove the card and reinsert it.

Figure 3-1 Inserting a PC-Cardbus Card into a Computer



Note The configuration profiles for PC-Cardbus cards are tied to the slot in which the card is inserted. Therefore, you must always insert your PC-Cardbus card into the same slot or create profiles for both slots. See Chapter 4 for information on creating profiles for your client adapter.

Step 4 If the Found New Hardware Wizard window appears, click **Cancel**.

Note If you do not click **Cancel**, the wizard will attempt to install software for the client adapter but will be unable to find it.

Step 5 Go to the "Installing the Client Adapter Software" section on page 3-9.

Inserting a PCI Card

You must perform the following procedures in the order listed below to insert a PCI card:

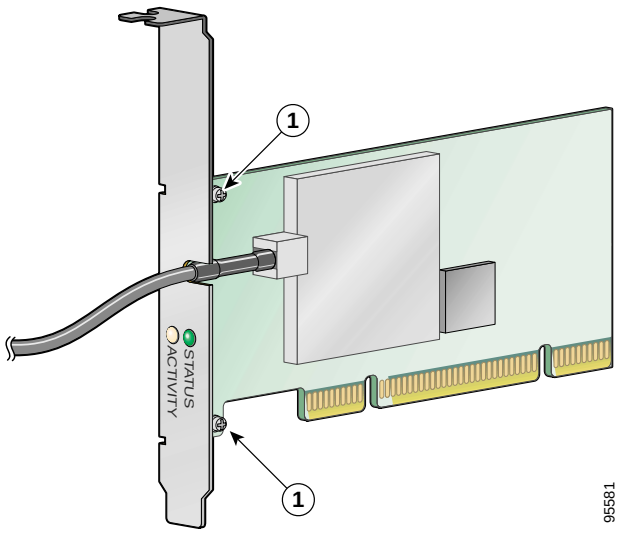
- Change the bracket (if required), see below
- Insert the card, page 3-4
- Assemble the antenna, page 3-5
- Mount the antenna, page 3-6

Changing the Bracket

The PCI card is shipped with a full-profile bracket attached. If the PC into which you are inserting the PCI card requires the card to use a low-profile bracket, follow these steps to change brackets.

Step 1 Remove the two screws that attach the bracket to the card. See Figure 3-2.

Figure 3-2 Changing the PCI Card Bracket



1	Bracket screws

Step 2 Slide the bracket away from the card; then tilt the bracket to free the antenna cable.

Caution Do not pull on the antenna cable or detach it from the PCI card. The antenna is meant to be permanently attached to the card.

Step 3 Hold the low-profile bracket to the card so that the LEDs slip through their corresponding holes on the bracket.

Step 4 Insert the screws that you removed in Step 1 into the holes on the populated side of the card near the bracket (see Figure 3-2) and tighten.

Inserting the Card

Follow the steps below to insert a PCI card into your PC.

Step 1 Turn off the PC and all its components.

Step 2 Remove the computer cover.

Note On most Pentium PCs, PCI expansion slots are white. Refer to your PC documentation for slot identification.

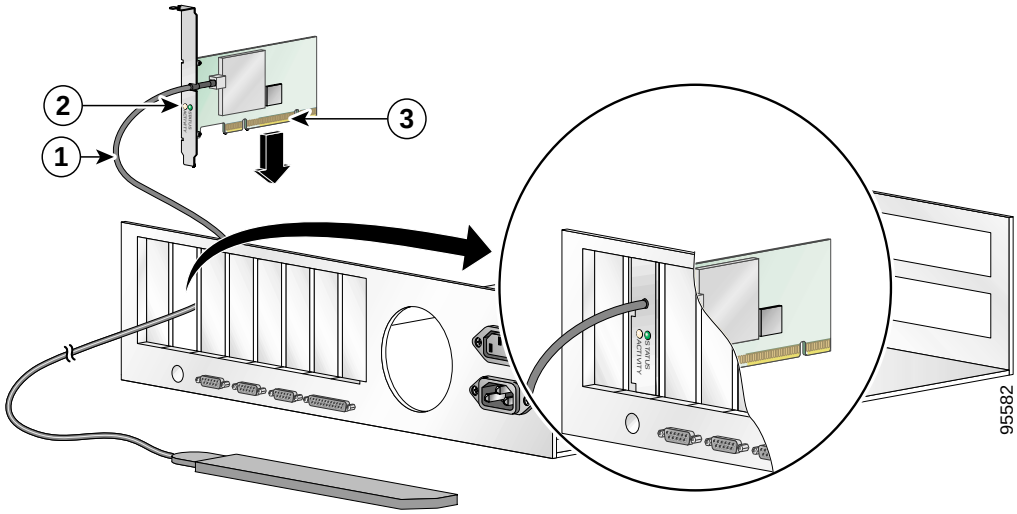
Step 3 Remove the screw from the top of the CPU back panel above an empty PCI expansion slot. This screw holds the metal bracket on the back panel.

Caution Static electricity can damage your PCI card. Before removing the card from the anti-static packaging, discharge static by touching a metal part of a grounded PC.

Step 4 Locate an empty PCI expansion slot inside your computer.

Step 5 Slip your card's antenna through the opening near the empty expansion slot so that it is located outside of the computer. See Figure 3-3.

Figure 3-3 Inserting a PCI Card into a PC



1	Antenna cable
2	LEDs
3	Card edge connector

Step 6 Tilt the card to enable the LEDs to slip through the opening in the CPU back panel. See the enlarged view in Figure 3-3.

Step 7 Press the card into the empty slot until its connector is firmly seated.

Caution Do not force the card into the expansion slot; this could damage both the card and the slot. If the card does not insert easily, remove it and reinsert it.

Step 8 Reinstall the screw on the CPU back panel and replace the computer cover.

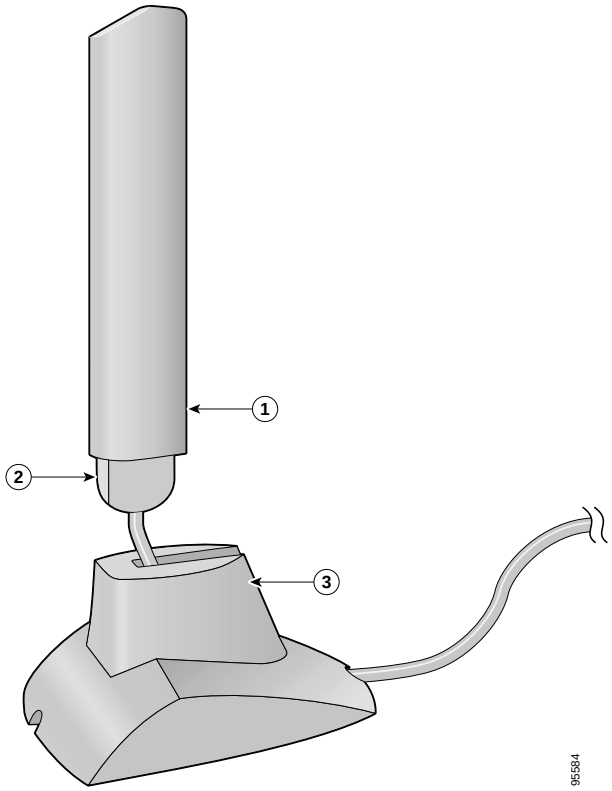
Assembling the Antenna

Follow the steps below to assemble the PCI card's antenna.

Step 1 Slide the antenna through the opening in the bottom of the antenna base.

Step 2 Position the antenna so its notches are facing the Cisco label on the front of the base. See Figure 3-4.

Figure 3-4 Inserting the Antenna into Its Base



1	Antenna
2	Notch
3	Antenna base

Step 3 Press the antenna cable into the receptacle on the top of the base as shown in Figure 3-4.

Step 4 Press the antenna straight down into the receptacle until it clicks into place.

Mounting the Antenna

Because the PCI card is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

- Place the PCI card's antenna in an area where large steel structures such as shelving units, bookcases, and filing cabinets will not obstruct radio signals being transmitted or received.
- Place the antenna away from microwave ovens and 2.4- and 5.8-GHz cordless phones. These products can cause signal interference because they operate in the same frequency range as the PCI card.

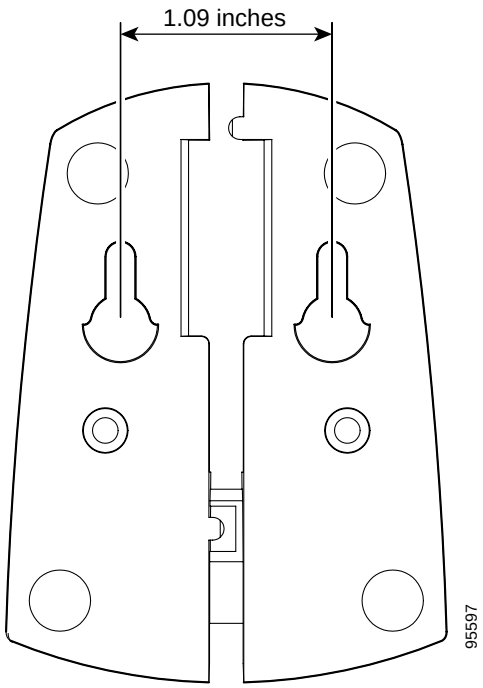
Follow the steps below to position the PCI card's antenna on a flat horizontal surface or to mount it to a wall.

Step 1 Perform one of the following:

- If you want to use the antenna on a flat horizontal surface, position the antenna so it is pointing straight up. Then go to Step 7.
- If you want to mount the antenna to a wall, go to Step 2.

Step 2 Drill two holes in the wall that are 1.09 in. (2.8 cm) apart. Figure 3-5 shows the distance between the mounting holes on the bottom of the antenna base.

Figure 3-5 Bottom of Antenna Base

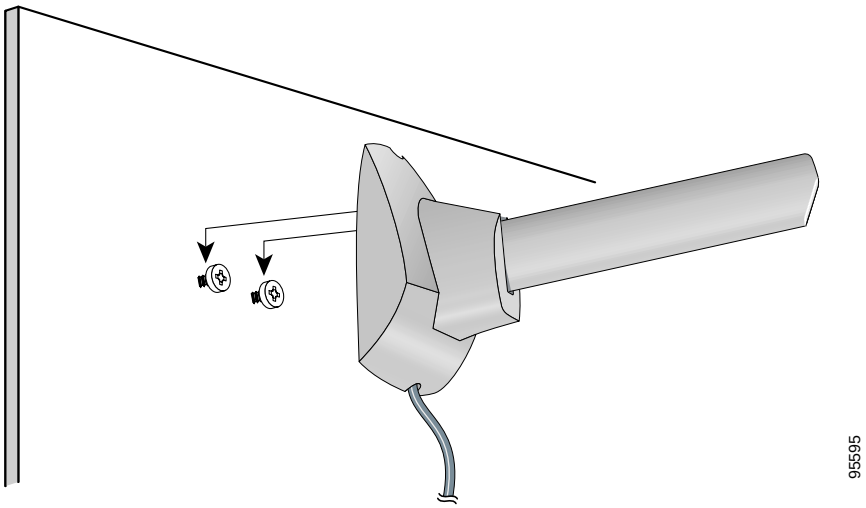


Step 3 Tap the two supplied wall anchors into the holes.

Step 4 Drive the two supplied screws into the wall anchors, leaving a small gap between the screw head and the anchor.

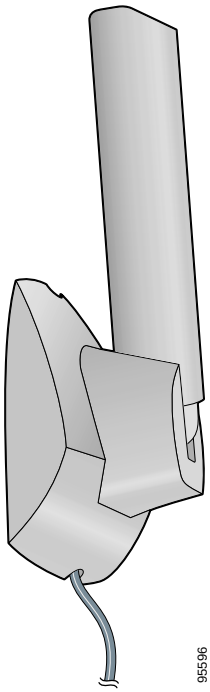
Step 5 Position the mounting holes on the bottom of the antenna base over the screws (see Figure 3-6) and pull down to lock in place.

Figure 3-6 Mounting the Antenna



Step 6 The antenna rotates 90 degrees from its base. For optimal reception, position the antenna so it is pointing straight up (see Figure 3-7).

Figure 3-7 Rotating the Antenna



Step 7 Boot up your PC. The green LED lights when the card is inserted properly.

Step 8 If the Found New Hardware Wizard window appears, click **Cancel**.

Step 9 Go to the "Installing the Client Adapter Software" section below.

Installing the Client Adapter Software

This section describes how to install Cisco Aironet CB21AG or PI21AG client adapter driver and utilities from a single executable file named *WinClient-802.11a-b-g-Ins-Wizard-vx.exe*, where *x* represents the release number. Follow these steps to install these client adapter software components on a computer running Windows 2000 or XP.

Caution Cisco Aironet CB21AG and PI21AG client adapter software is incompatible with other Cisco Aironet client adapter software. The Aironet Desktop Utility (ADU) must be used with CB21AG and PI21AG cards, and the Aironet Client Utility (ACU) must be used with all other Cisco Aironet client adapters.

Caution Do not eject your client adapter at any time during the installation process, including during the reboot.

Note This procedure is meant to be used the first time the Cisco Aironet CB21AG or PI21AG client adapter software is installed on your computer. If this software is already installed on your computer, follow the instructions in Chapter 9 to upgrade the client adapter software.

Note Only one wireless client adapter can be installed and used at a time. The software does not support the use of multiple cards.

Step 1 Make sure the client adapter is inserted in your computer.

Note If your client adapter is not inserted, the software cannot be installed.

Step 2 Use your computer's web browser to access the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

Step 3 Click **Option #2: Aironet Wireless Software Display Tables**.

Note If you prefer to use an automated tool, you can download software from the Software Selector tool instead of the display tables. To do so, click **Option #1: Aironet Wireless Software Selector**, follow the instructions on the screen, and go to Step 7.

Step 4 Click **Cisco Aironet Wireless LAN Client Adapters**.

Step 5 Under Aironet Client Adapter Installation Wizard (For Windows), click **802.11a/b/g (CB21AG, PI21AG)**.

Step 6 Click the Install Wizard file with the greatest release number.

Step 7 Complete the encryption authorization form; then read and accept the terms and conditions of the Software License Agreement.

Step 8 Click the file again to download it.

Step 9 Save the file to your computer's hard drive.

Step 10 Use Windows Explorer to find the file.

Step 11 Double-click the file. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see Figure 3-8) and the Cisco Aironet Installation Program window (see Figure 3-9).

Figure 3-8 Preparing Setup Window

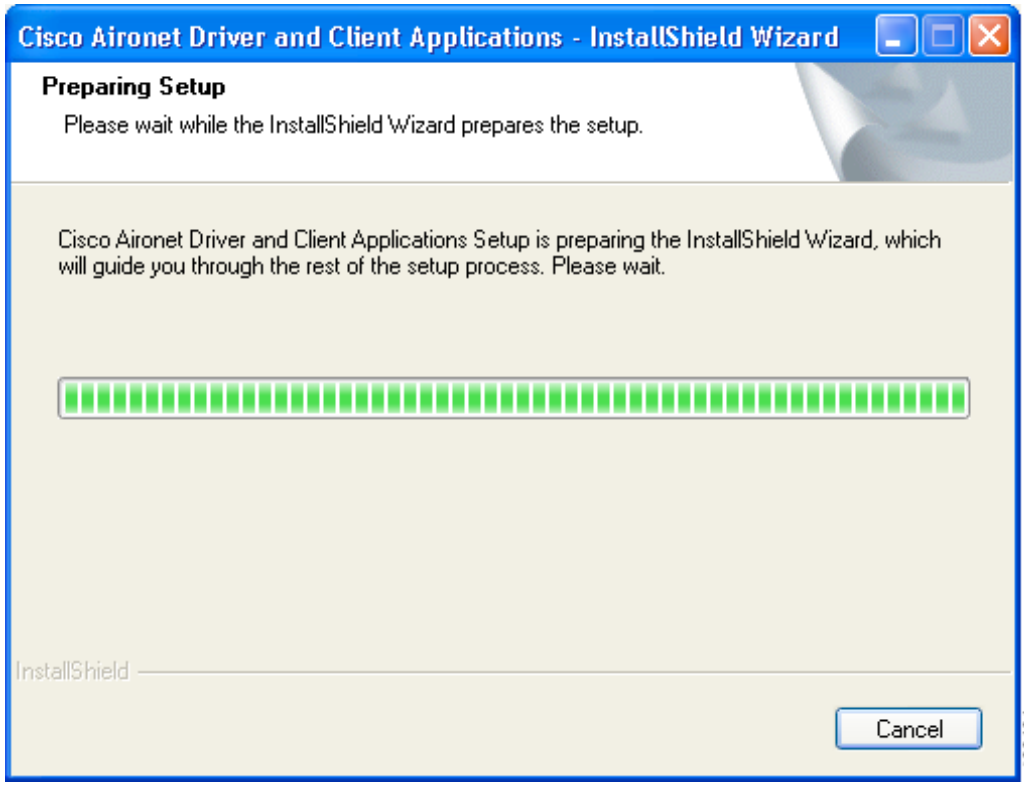
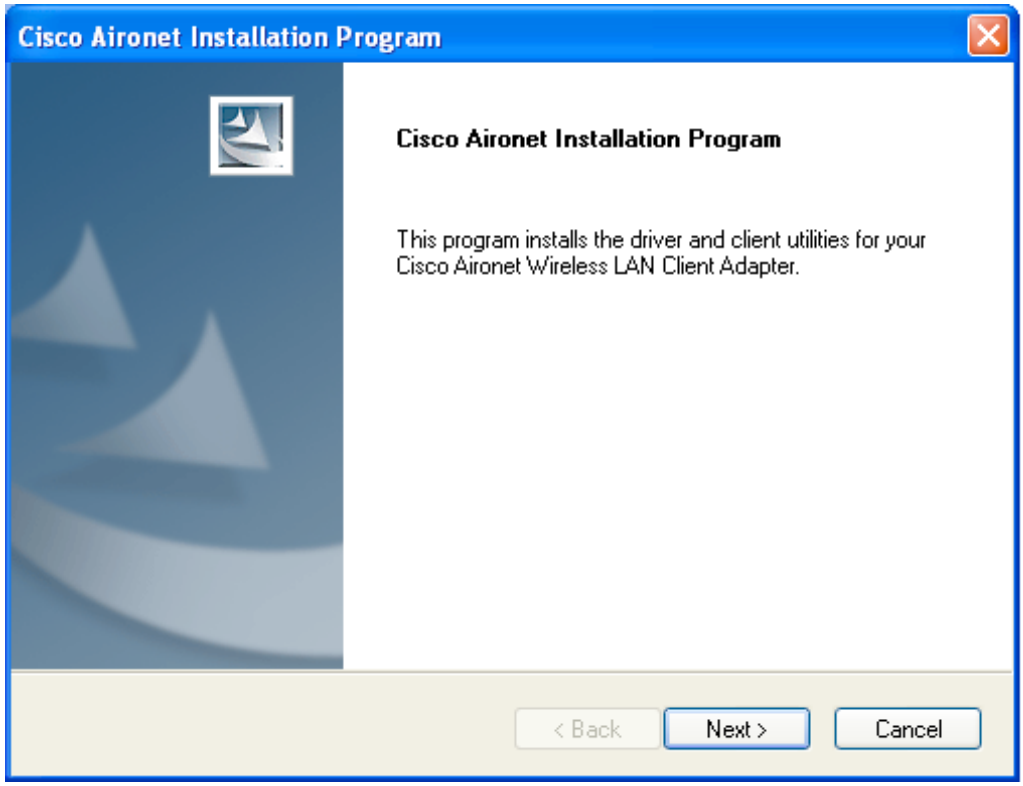
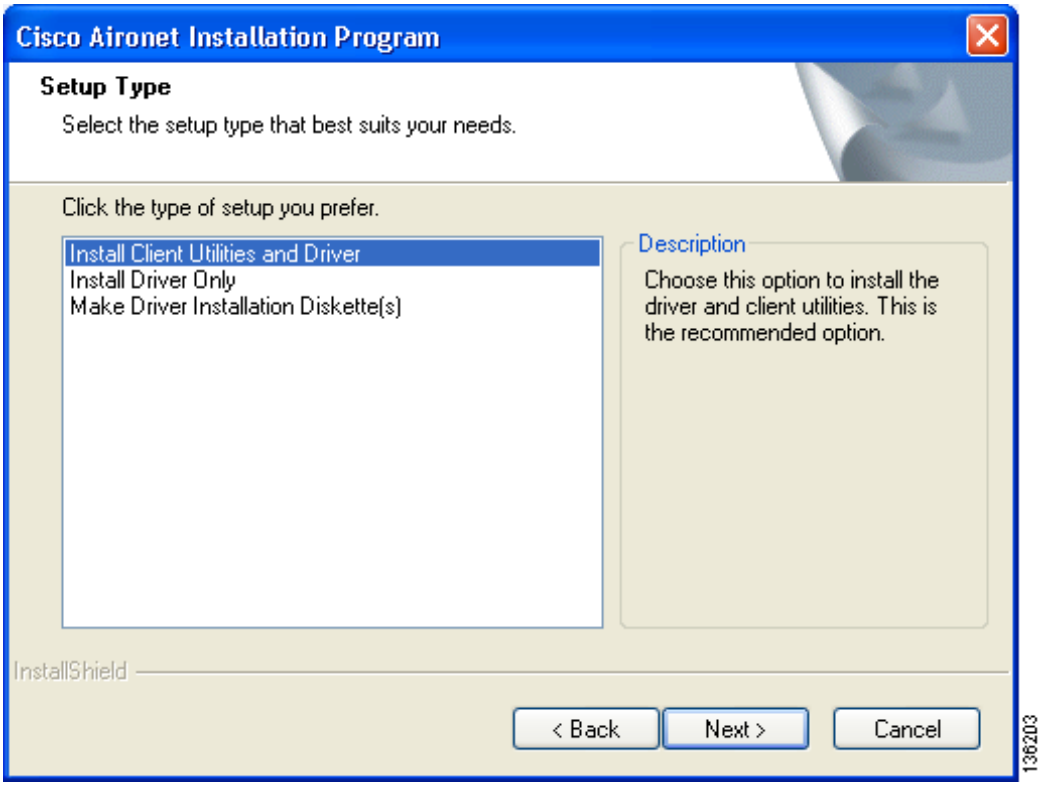


Figure 3-9 Cisco Aironet Installation Program Window



Step 12 Click **Next**. The Setup Type window appears (see Figure 3-10).

Figure 3-10 Setup Type Window



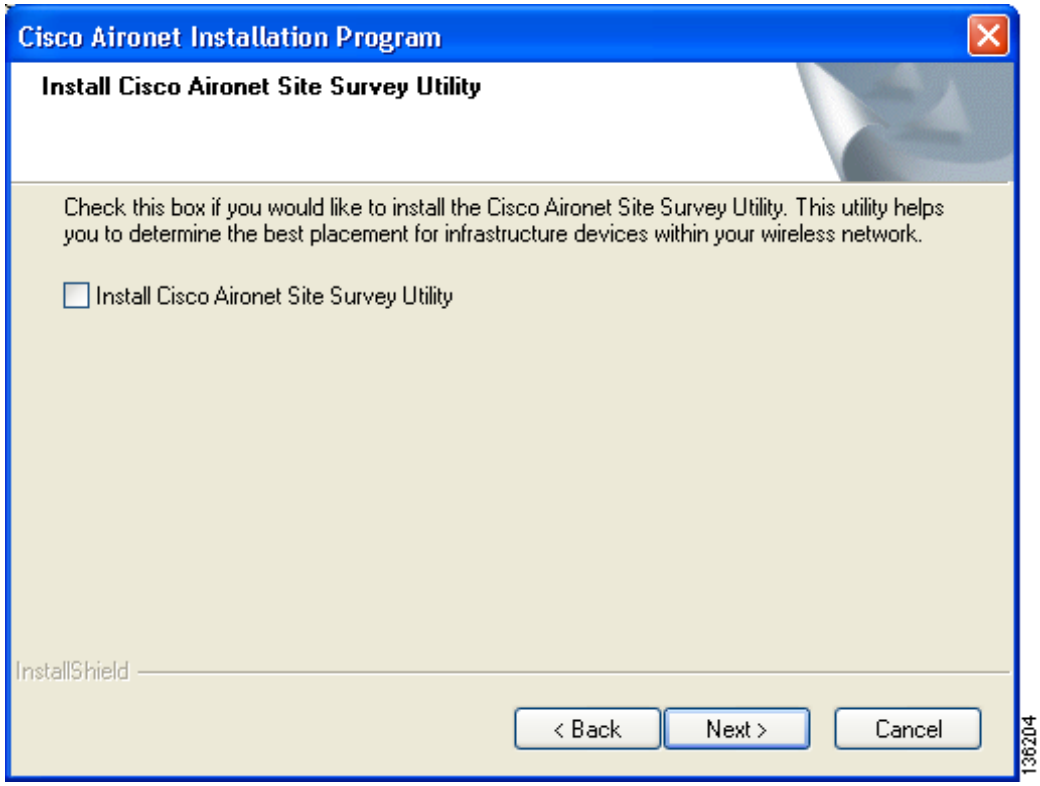
Step 13 Choose one of the following options:

Note To ensure compatibility among software components, Cisco recommends that you install the client utilities and driver.

- **Install Client Utilities and Driver**—Installs the client adapter driver and client utilities.
- **Install Driver Only**—Installs only the client adapter driver. If you choose this option, click **Next** and go to Step 26.
- **Make Driver Installation Diskette(s)**—Enables you to create driver installation diskettes that can be used to install drivers using the Windows Device Manager.

Step 14 Click **Next**. The Install Cisco Aironet Site Survey Utility window appears (see Figure 3-11).

Figure 3-11 Install Cisco Aironet Site Survey Utility Window



Step 15 Check the **Install Cisco Aironet Site Survey Utility** check box if you want to install a utility that helps you to determine the best placement of infrastructure devices within your wireless network. Click **Next**.

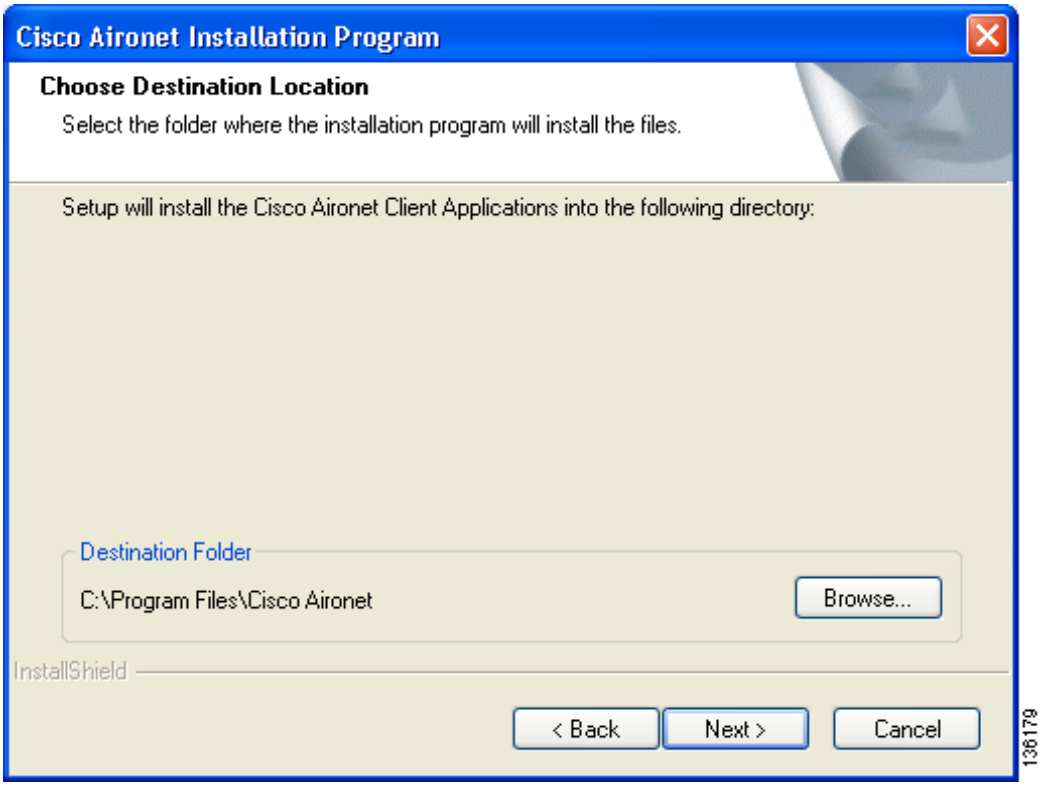
Note The site survey utility is a stand-alone application, separate from ADU, that runs from an executable file. If you check the Install Site Survey Utility check box, the Install Wizard installs the site survey executable file in the C:\Program Files\Cisco Aironet directory (unless you specify a different directory in Step 17). See Appendix F for instructions on using the utility.

Step 16 If a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.

Note If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.

The Choose Destination Location window appears (see Figure 3-12).

Figure 3-12 Choose Destination Location Window



Step 17 Perform one of the following:

- If you chose the first option in Step 13, click **Next** to install the client utility files in the C:\Program Files\Cisco Aironet directory.

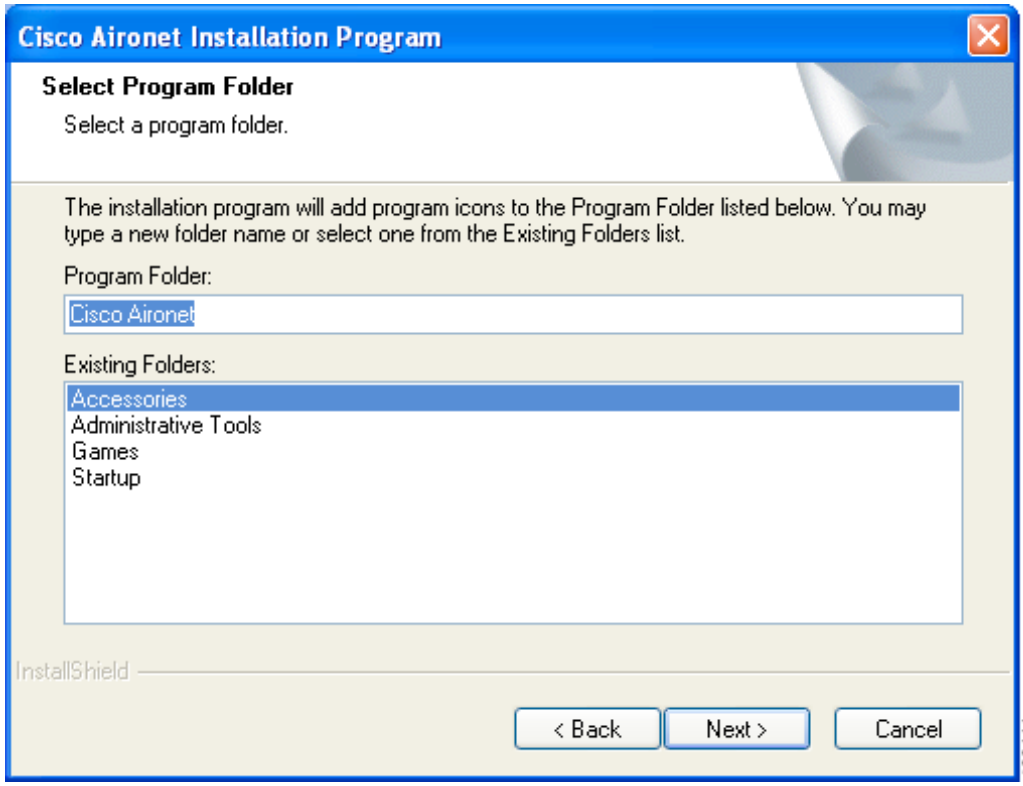
  Note If you want to install the client utilities in a different directory, click **Browse**, choose a different directory, click **OK**, and click **Next**.

- If you chose the Make Driver Installation Diskette(s) option in Step 13, insert a floppy disk into your computer and click **Next** to copy the driver to the diskette. Go to Step 26.

  Note If you want to copy the driver to a different drive or directory, click **Browse**, choose a new location, click **OK**, and click **Next**.

Step 18 The Select Program Folder window appears (see Figure 3-13).

Figure 3-13 Select Program Folder Window

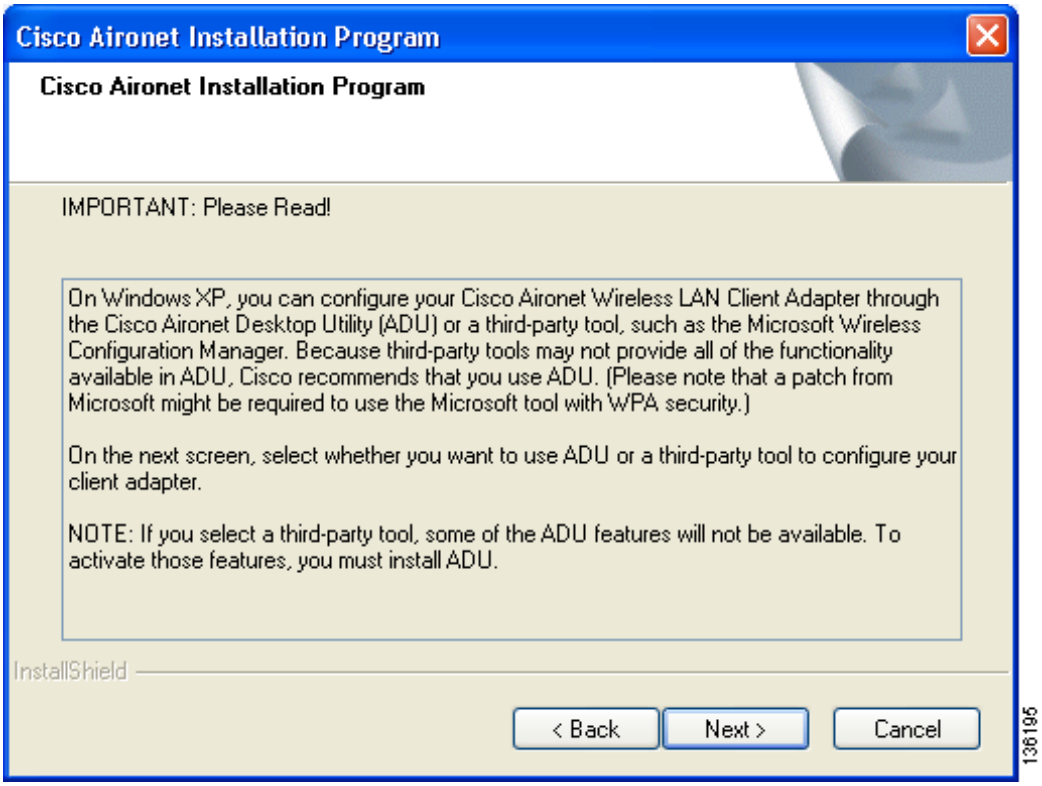


Step 19 Click **Next** to add program icons to the Cisco Aironet program folder.

Note If you want to specify a different program folder, choose a folder from the Existing Folders list or type a new folder name in the Program Folder field and click **Next**.

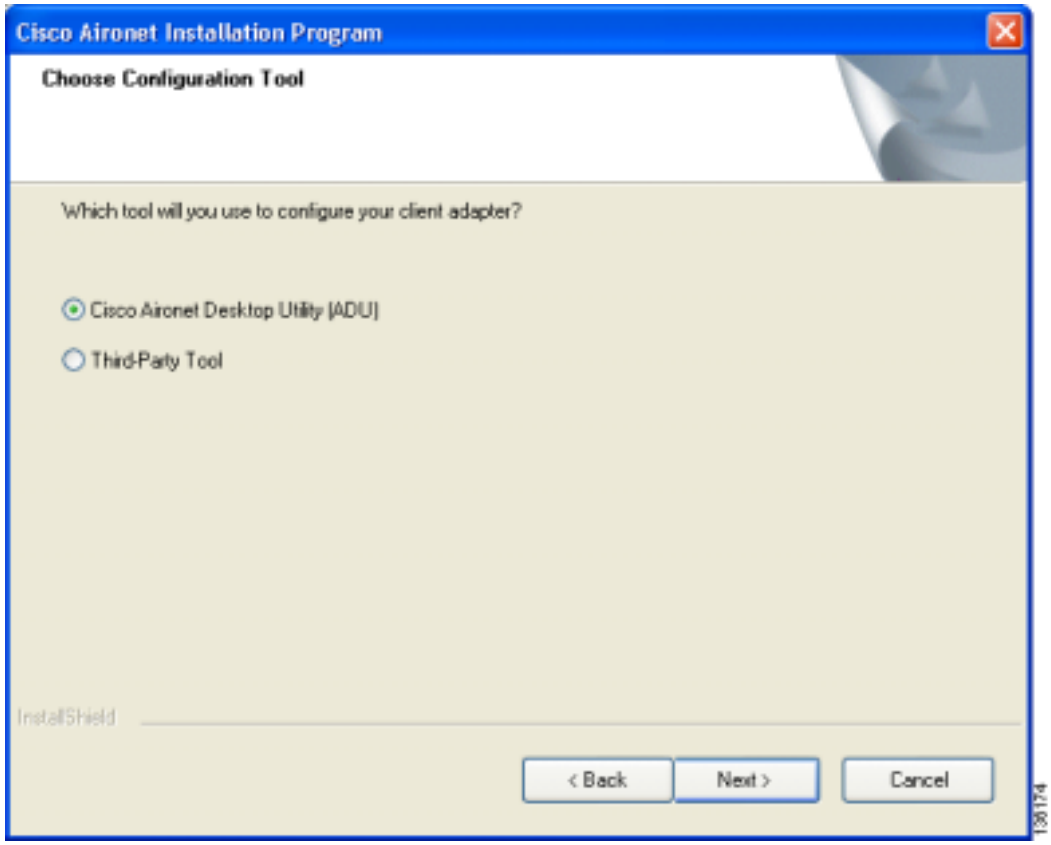
Step 20 If your computer is running Windows 2000, go to Step 26. If your computer is running Windows XP, the IMPORTANT: Please Read! window appears (see Figure 3-14).

Figure 3-14 IMPORTANT: Please Read! Window



Step 21 Read the information displayed and click **Next**. The Choose Configuration Tool window appears (see Figure 3-15).

Figure 3-15 Choose Configuration Tool Window



Step 22 Choose one of the following options:

- **Cisco Aironet Desktop Utility (ADU)**—Enables you to configure your client adapter using ADU.
- **Third-Party Tool**—Enables you to configure your client adapter using a third-party tool such as the Microsoft Wireless Configuration Manager in Windows XP.

Table 3-1 compares Windows XP and ADU client adapter features.

Table 3-1 Comparison of Windows XP and ADU Client Adapter Features

Feature	Windows XP	ADU
Configuration parameters	Limited	Extensive
Capabilities		
Create profiles	Yes	Yes
Enable/disable radio	No	Yes

Table 3-1 Comparison of Windows XP and ADU Client Adapter Features

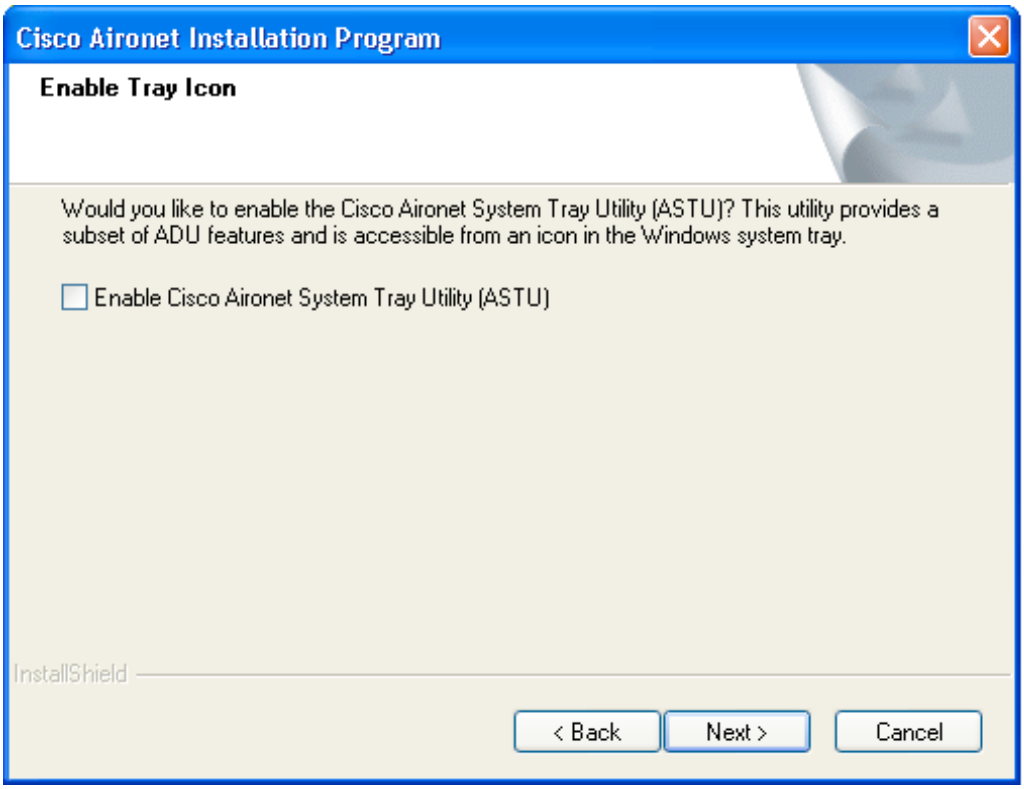
Feature	Windows XP	ADU
Security		
Static WEP	Yes	Yes
LEAP or EAP-FAST authentication with dynamic WEP	No	Yes
EAP-TLS or PEAP authentication	Yes	Yes
Status and statistics		
Status window	Limited	Extensive
Statistics window (transmit & receive)	No	Yes

Note If you choose Cisco Aironet Desktop Utility (ADU) above, the Microsoft Wireless Configuration Manager is disabled. If you ever manually enable it, you are prompted to disable it whenever ADU is activated.

Step 23 Click **Next**.

Step 24 If you chose Cisco Aironet Desktop Utility (ADU) in Step 22, go to Step 26. If you chose Third-Party Tool, the Enable Tray Icon window appears (see Figure 3-16).

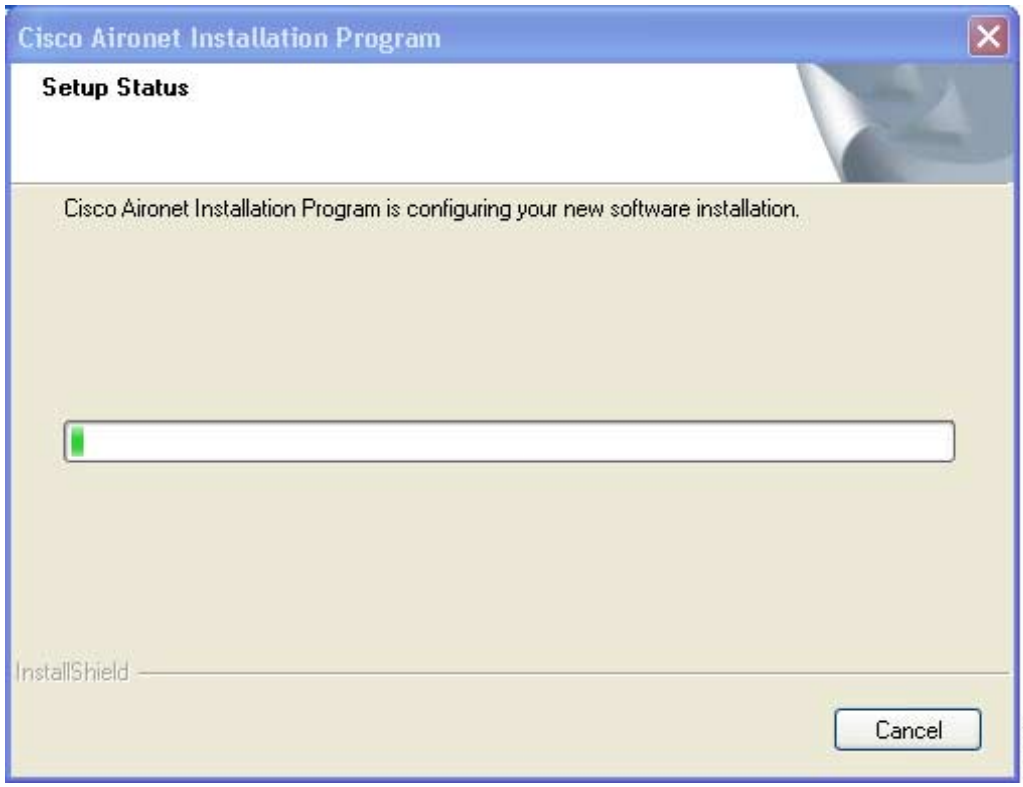
Figure 3-16 Enable Tray Icon Window



Step 25 Check the **Enable Cisco Aironet System Tray Utility (ASTU)** check box if you want to be able to use ASTU even though you have chosen to configure your client adapter through a third-party tool instead of ADU and click **Next**.

Step 26 When prompted to insert your client adapter, click **OK**. The Setup Status window appears (see Figure 3-17).

Figure 3-17 Setup Status Window



The installation process begins, and you are notified as each software component is installed.

Step 27 When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart.

Step 28 If the Windows Found New Hardware Wizard appears after your computer reboots, click **Next**, allow the wizard to install the software for the client adapter, and click **Finish**.

Step 29 If your network setup does not include a DHCP server and you plan to use TCP/IP, follow these steps for your operating system.

- **Windows 2000**
  - **a.** Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.
  - **b.** Right-click **Local Area Connection *x*** (where *x* represents the number of the connection).
  - **c.** Click **Properties**.
  - **d.** In the Components Checked Are Used by This Connection field, click **Internet Protocol (TCP/IP)** and **Properties**.

e. Choose **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator).

f. Click **OK** to close each open window.

- **Windows XP**

a. Double-click **My Computer**, **Control Panel**, and **Network Connections**.

b. Right-click **Wireless Network Connection *x*** (where *x* represents the number of the connection).

c. Click **Properties**.

d. In the This Connection Uses the Following Items field, click **Internet Protocol (TCP/IP)** and **Properties**.

e. Choose **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator).

f. Click **OK** to close each open window.

Step 30 If you are prompted to restart your computer, click **Yes**.

Step 31 Now that your client adapter is properly installed, it is ready to be configured.

- If you are planning to configure your client adapter through ADU, go to Chapter 4 to create configuration profiles.
- If you are planning to configure your client adapter through the Windows XP Wireless Configuration Manager, go to Appendix E.
- If you are planning to configure your client adapter through another third-party tool, refer to the documentation for that application.

Note If you want to be able to use ADU's Group Policy Delay parameter, follow the instructions below to download and install a necessary hot fix before configuring your client adapter.

Note If you experienced problems during or after installation, refer to Chapter 10 for troubleshooting information.

Installing a Microsoft Hot Fix for Group Policy Delay

If you want to use the Group Policy Delay parameter on the Profile Management (Security) window in ADU, you must install a Microsoft hot fix on computers running Windows 2000. The hot fix is incorporated into Windows XP Service Pack 2 and later.

The Group Policy Delay parameter enables you to specify how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. Follow the steps below to obtain and install the hot fix.

Note You must be a registered Cisco customer and log into Cisco.com in order to download the hot fix. If you are unable to access the hot fix from Cisco.com, contact Microsoft Support to obtain it. The Windows 2000 support page provides the contact information: http://support.microsoft.com/oas/default.aspx?&c1=508&gprid=7274&

Step 1 Use your computer's web browser to access the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/aironet_hotfix

Step 2 Click the hot fix file (userenv.zip).

Step 3 Complete the encryption authorization form and click **Submit**.

Step 4 Click the file again to download it.

Step 5 Save the file to your computer's hard drive.

Step 6 Find the file using Windows Explorer, double-click it, and extract its files to a folder.

Step 7 Reboot your computer and press **F8** while your computer is booting.

Step 8 When the boot menu appears, select **Safe Mode with Command Prompt**.

Note You must complete this procedure in safe mode; otherwise, system file protection (SFP) will silently restore the original version of the file you are replacing.

Step 9 Copy the hot fix file (userenv.dll) to %systemroot%\System32 and overwrite the existing version of this file.

Step 10 Delete the copy of userenv.dll in %systemroot%\System32\DllCache.

Step 11 Reboot your computer.

CHAPTER 4

Using the Profile Manager

This chapter explains how to use the ADU profile manager feature to create and manage profiles for your client adapter.

The following topics are covered in this chapter:

- Overview of Profile Manager, page 4-2
- Opening Profile Manager, page 4-2
- Creating a New Profile, page 4-4
- Including a Profile in Auto Profile Selection, page 4-7
- Selecting the Active Profile, page 4-9
- Modifying a Profile, page 4-10
- Importing and Exporting Profiles, page 4-10

Overview of Profile Manager

The ADU profile manager feature enables you to create and manage up to 16 *profiles* (or saved configurations) for your client adapter. These profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for using your client adapter at the office, at home, and in public areas such as airports. After the profiles are created, you can easily switch between them without having to reconfigure your client adapter each time you enter a new location.

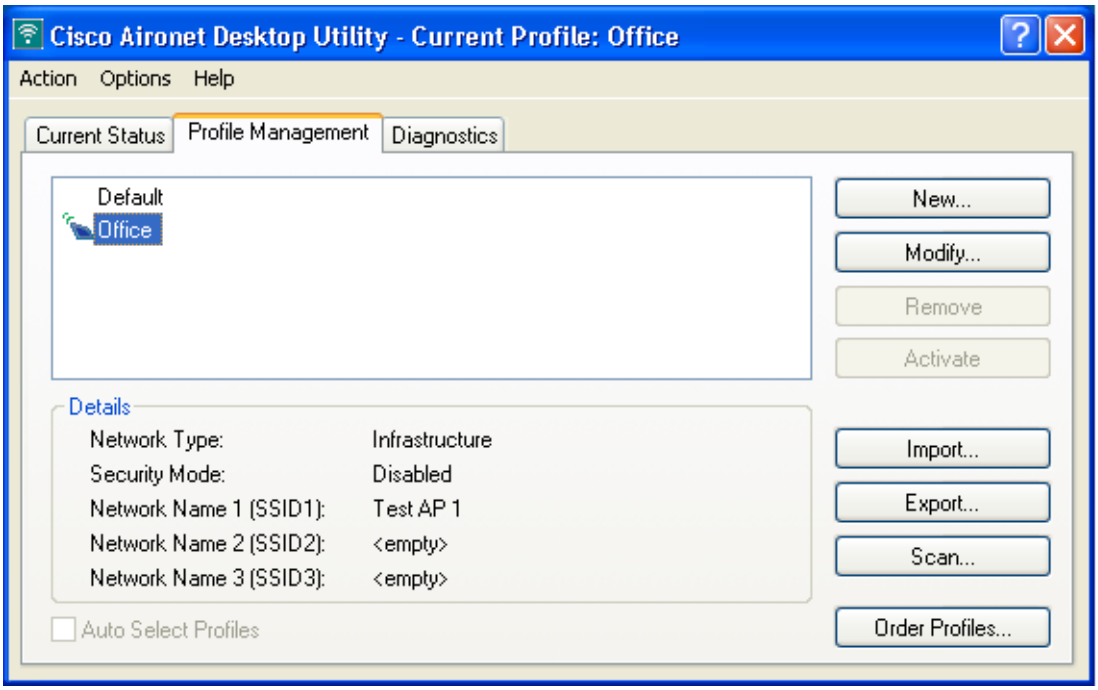
Profiles are stored in the registry and are lost if you uninstall the client adapter's software. To prevent your profiles from becoming lost, Cisco recommends that you back up your profiles using the profile manager's import/export feature. See the "Importing and Exporting Profiles" section on page 4-10 for details.

Opening Profile Manager

Step 1 To open the ADU profile manager, double-click the **Aironet Desktop Utility** icon on your desktop.

Step 2 Click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Figure 4-1 Cisco Aironet Desktop Utility (Profile Management) Window



Note The profile manager feature provides you with a default profile that is configured to use default values. This profile is named *Default* and appears in the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window. You can use this profile as is by double-clicking it or modify it by following the instructions in the "Modifying a Profile" section on page 4-10.

Table 4-1 provides a description of the status fields on the Cisco Aironet Desktop Utility (Profile Management) window.

Table 4-1 Description of Status Fields on Profile Management Window

Field	Description
Network Type	The type of network that is configured for the selected profile. **Value:** Infrastructure or Ad Hoc **Note** Refer to the Network Type parameter in Table 5-3 for instructions on setting the network type.
Security Mode	The type of security that is configured for the selected profile. **Value:** None, Pre-Shared Key, WPA/WPA2 Passphrase, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP **Note** Refer to Chapter 5 for instructions on setting client adapter security.
Network Name 1 (SSID1)	The service set identifier (SSID) is the wireless network that is configured for the selected profile. **Note** Refer to the SSID1 parameter in Table 5-2 for instructions on setting SSID1.
Network Name 2 (SSID2)	An optional SSID that is configured for the selected profile. It identifies a second distinct network and enables the client adapter to connect and/or roam to that network without having to be reconfigured. **Note** Refer to the SSID2 parameter in Table 5-2 for instructions on setting SSID2.
Network Name 3 (SSID3)	An optional SSID that is configured for the selected profile. It identifies a third distinct network and enables the client adapter to connect and/or roam to that network without having to be reconfigured. **Note** Refer to the SSID3 parameter in Table 5-2 for instructions on setting SSID3.

Profile manager enables you to perform the following tasks related to the management of profiles:

- Create a new profile, page 4-4
- Include a profile in auto profile selection, page 4-7
- Select the active profile, page 4-9
- Edit a profile, page 4-10
- Delete a profile, page 4-10
- Import a profile, page 4-11
- Export a profile, page 4-11

Follow the instructions on the page indicated for the task you want to perform.

Note If your system administrator used an administrative tool to deactivate certain parameters, these parameters are disabled and cannot be selected.

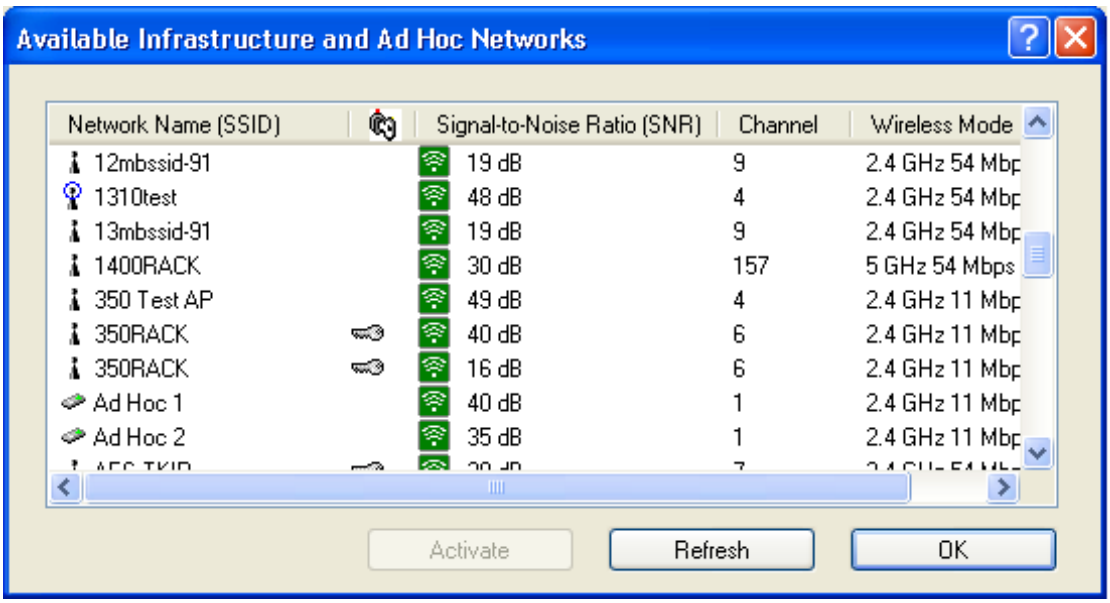
Creating a New Profile

Follow the steps below to create a new profile.

Step 1 Perform one of the following:

- If you want to create a new profile from scratch, click **New** on the Cisco Aironet Desktop Utility (Profile Management) window. Then go to Step 4.
- If you want to find an available network and create a profile based on it, click **Scan** on the Cisco Aironet Desktop Utility (Profile Management) window. The Available Infrastructure and Ad Hoc Networks window appears (see Figure 4-2).

Figure 4-2 Available Infrastructure and Ad Hoc Networks Window



This window displays a list of all available networks. Click the **Refresh** button when you want to refresh the window and update the list of available networks.

Note The SSID of a Cisco IOS access point appears in the list of available networks only if a Guest Mode SSID is enabled or the Broadcast SSID in Beacon option is selected. Refer to the software configuration guide for your access point for additional information.

Table 4-2 provides a description of the fields on the Available Infrastructure and Ad Hoc Networks window.

Table 4-2 Description of Fields on Available Infrastructure and Ad Hoc Networks Window

Field	Description
Network Name (SSID)	The service set identifier (SSID) indicates the name of an available wireless network. The icons to the left of the SSIDs provide information on network type and link status.
	Icon / **Description**: An available infrastructure network.
	The infrastructure network to which your client adapter is currently associated.
	An available ad hoc network.
	The ad hoc network to which your client adapter is currently associated.
Key icon	SSIDs that are designated with a key icon are being advertised as secure networks.
Signal-to-Noise Ratio (SNR)	The difference between the signal strength and the current noise level. The higher the value, the better the client adapter's ability to communicate with the access point. **Note** The color of this parameter's icon provides a visual interpretation of the signal-to-noise ratio: Excellent or Good (green), Fair (yellow), Poor (red). **Note** The signal-to-noise ratio is displayed either in decibels (dB) or as a percentage (%), depending on the value selected for the Signal Strength Display Units parameter on the Display Settings window. See the "Setting Parameters that Affect ADU Status and Statistics Tools" section on page 7-2 for more information.
Channel	The channel that the access point (in infrastructure mode) or the other client (in ad hoc mode) is using for communications.
Wireless Mode	The frequency and rate at which the access point (in infrastructure mode) or the other client (in ad hoc mode) is configured to transmit and receive packets.

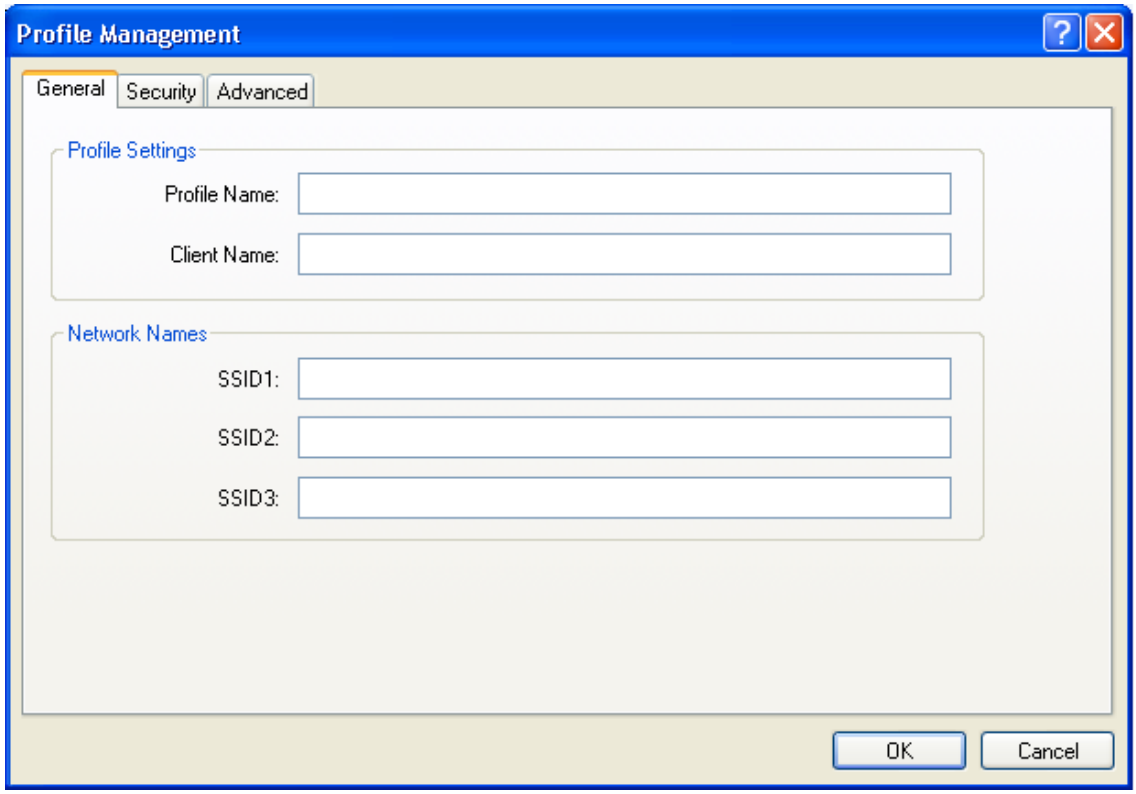
Step 2 Scroll down to see the full list of available networks.

Step 3 Click the SSID of the network to which you want your client adapter to associate and click **Activate**.

Note If the SSID is blank, you cannot activate the network.

Step 4 When the Profile Management (General) window appears (see Figure 4-3), enter a name for your new profile (such as *Office*, *Home*, etc.) in the Profile Name field.

Figure 4-3 Profile Management (General) Window



Note If you are creating a profile after scanning for an available network, the SSID of the network appears in the SSID1 field.

Step 5 Perform one of the following:

- If you want this profile to use the default values, click **OK**. The profile is added to the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window.
- If you want to change any of the configuration parameter settings, follow the instructions in Chapter 5. The profile is added to the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window.

Note The profiles for PC-Cardbus cards are tied to the slot in which the card is inserted. Therefore, you must always insert your PC-Cardbus card into the same slot, create profiles for both slots, or export the profiles from one slot and import them for the other slot.

Step 6 Go to the "Including a Profile in Auto Profile Selection" section on page 4-7 to enable the profile to be selected automatically or go to the "Selecting the Active Profile" section on page 4-9 to activate the profile.

Including a Profile in Auto Profile Selection

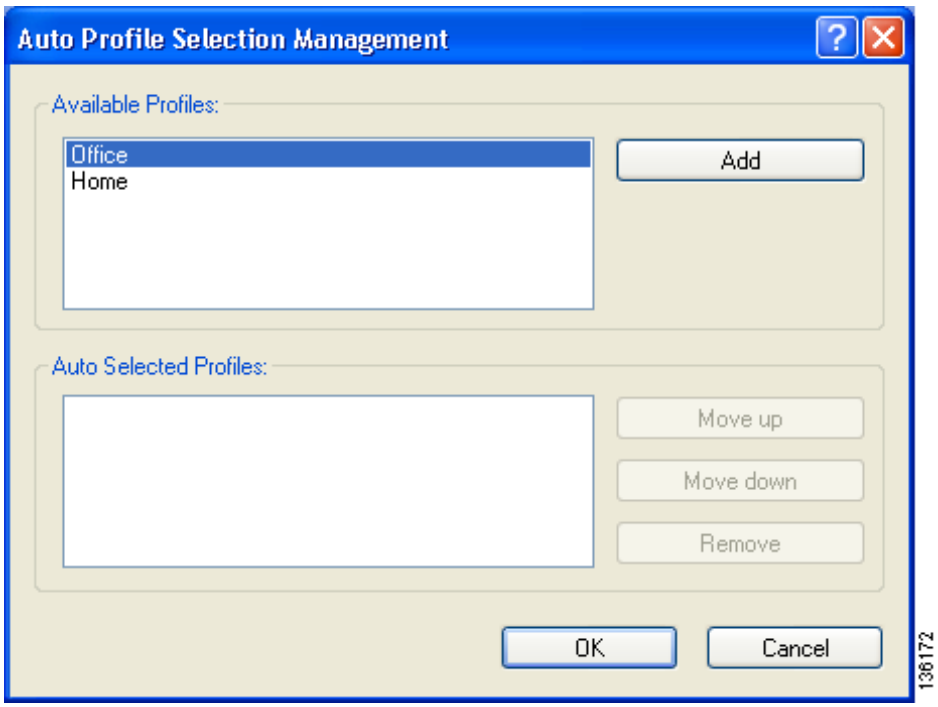
After you have created profiles for your client adapter, you can choose to include them in the profile manager's auto profile selection feature. Then when auto profile selection is enabled, the client adapter automatically selects a profile from the list of profiles that were included in auto profile selection and uses it to establish a connection to the network.

Follow these steps to include any of your profiles in auto profile selection and to establish the order in which the profiles will be selected for use.

Step 1 Open ADU and click the **Profile Management** tab.

Step 2 Click **Order Profiles**. The Auto Profile Selection Management window appears (see Figure 4-4).

Figure 4-4 Auto Profile Selection Management Window



Step 3 The profiles that you created are listed in the Available Profiles box. Highlight each one that you want to include in auto profile selection and click the **Add** button. The profiles appear in the Auto Selected Profiles box.

The following rules apply to auto profile selection:

- You must include at least two profiles in the Auto Selected Profiles box.
- The profiles must specify an SSID; otherwise, they do not appear in the Available Profiles box.
- Profiles cannot specify multiple SSIDs; otherwise, they do not appear in the Available Profiles box.
- Each profile that is included in auto profile selection must have a unique SSID. For example, if Profile A and Profile B both have "ABCD" as their SSID, only Profile A or Profile B (whichever was created first) appears in the Available Profiles box and can be included in auto profile selection.

Note To remove a profile from auto profile selection, select the profile in the Auto Selected Profiles box and click **Remove**. The profile is removed from the Auto Selected Profiles box.

Step 4 The first profile in the Auto Selected Profiles box has the highest priority while the last profile has the lowest priority. To change the order (and priority) of your auto-selectable profiles, select the profile that you want to move and click **Move up** or **Move down** to move the profile up or down, respectively.

Step 5 Click **OK** to save your changes.

When auto profile selection is enabled (see the "Selecting the Active Profile" section on page 4-9 for instructions), the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID and so on.

Note When you enable auto profile selection, the client adapter scans all wireless modes (5 GHz, 54 Mbps; 2.4 GHz, 11 Mbps; and 2.4 GHz, 54 Mbps) for an available network. The client ignores the selected profile's wireless mode setting, which was configured on the ADU Profile Management (Advanced) window. Using this method, the client does not need to drop the current connection nor change the current profile while looking for networks in other profiles.

Step 6 Go to the "Selecting the Active Profile" section on page 4-9 to enable auto profile selection.

Selecting the Active Profile

Follow the steps below to specify the profile that the client adapter is to use.

Note You can use ASTU instead of the ADU Profile Manager to select the active profile. Refer to Chapter 8 for instructions.

Step 1 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 2 Perform one of the following:

- Select one profile for the client adapter to use either by double-clicking that profile in the profiles list or by clicking that profile in the profiles list and then clicking **Activate**.

  If the client adapter cannot *associate* (or establish a connection) to an access point (in infrastructure mode) or another client (in ad hoc mode) or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To associate, you must select a different profile or enable auto profile selection.

- Enable auto profile selection by checking the **Auto Select Profiles** check box.

  This option causes the client adapter's driver to automatically select a profile from the list of profiles that were set up to be included in auto profile selection.

  If the client adapter loses association for more than 10 seconds (or for more than the time specified by the LEAP/EAP-FAST authentication timeout value on the LEAP/EAP-FAST Settings window if LEAP/EAP-FAST is enabled), the driver switches automatically to another profile that is included in auto profile selection. The adapter does not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP/EAP-FAST authentication timeout value). To force the client adapter to associate to a different access point (in infrastructure mode) or another client (in ad hoc mode), you must uncheck the **Auto Select Profiles** check box and select a new profile from the profiles list.

  Note This option is available only if two or more profiles are included in auto profile selection.

  Note Login scripts are not reliable if you use auto profile selection with LEAP or EAP-FAST. If you authenticate and achieve full network connectivity before or at the same time as you log into the computer, login scripts will run. However, if you authenticate and achieve full network connectivity after you log into the computer, login scripts will not run.

- Click **Scan**. The Available Infrastructure and Ad Hoc Networks window appears (see Figure 4-2). Double-click the SSID of a network that is used by one of your profiles and click **OK**.

The client adapter starts using a profile based on the option selected above. The active profile is designated by the following icon in the profiles list:

Modifying a Profile

Follow the steps in the appropriate section below to edit or delete an existing profile.

Editing a Profile

Step 1 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 2 In the profiles list, select the profile that you want to edit.

Step 3 Click **Modify**.

Step 4 Follow the instructions in Chapter 5 to change any of the configuration parameters for this profile.

Deleting a Profile

Step 1 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 2 In the profiles list, select the profile that you want to delete.

Note You cannot delete the active profile.

Step 3 Click **Remove**. The profile is deleted.

Importing and Exporting Profiles

This section provides instructions for importing and exporting profiles. You may want to use the import/export feature for the following reasons:

- To back up profiles before uninstalling client adapter software
- To export profiles for a PC-Cardbus card in one Cardbus slot and import them for use with a second Cardbus slot
- To set up your computer with a profile from another computer
- To export one of your profiles and use it to set up additional computers

Follow the instructions on the following pages to import or export profiles.

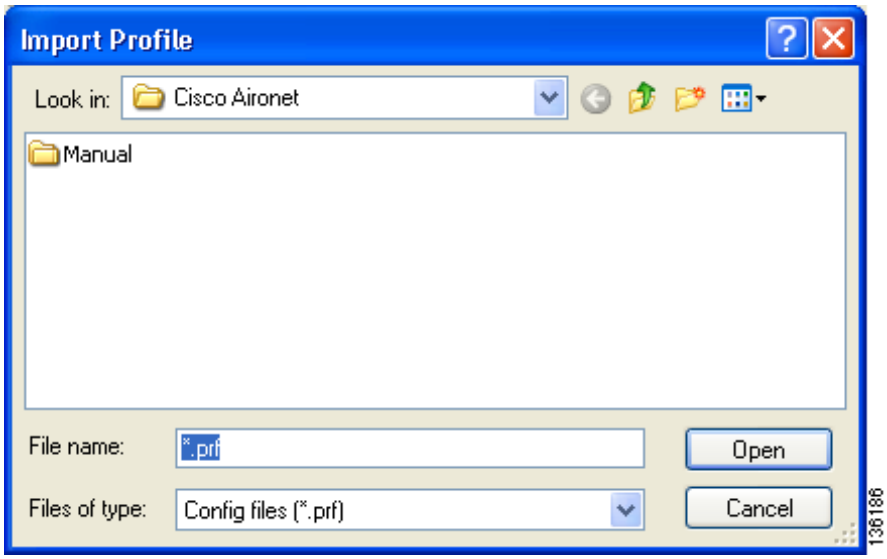
Importing a Profile

Step 1 If the profile that you want to import is on a floppy disk, insert the disk into your computer's floppy drive.

Step 2 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 3 Click **Import**. The Import Profile window appears (see Figure 4-5).

Figure 4-5 Import Profile Window



Step 4 In the Look in drop-down box, find the directory containing the profile.

Step 5 Select the profile that you want to import so it appears in the File name box at the bottom of the window.

Step 6 Click **Open**. The imported profile appears in the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window.

Exporting a Profile

Note PACs are not exported with EAP-FAST profiles.

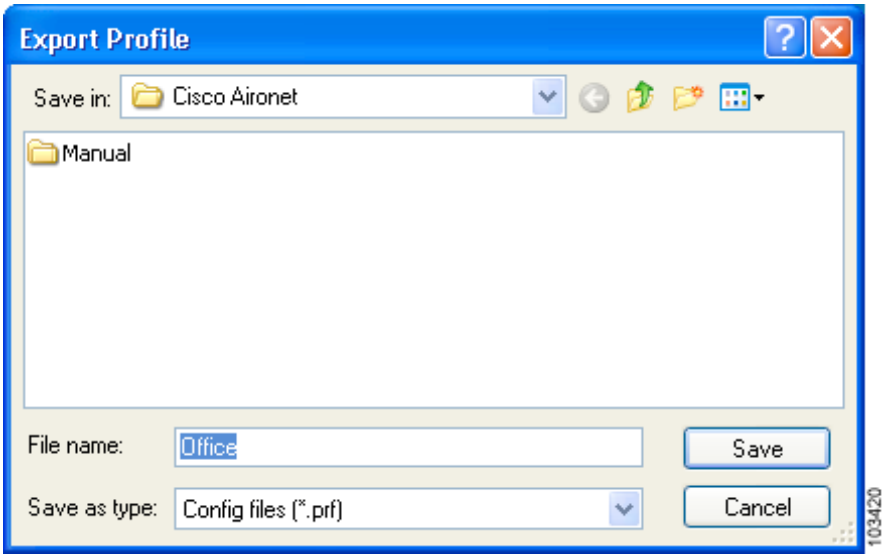
Step 1 Insert a blank floppy disk into your computer's floppy drive, if you wish to export a profile to a floppy disk.

Step 2 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 3 In the profiles list, select the profile that you want to export.

Step 4 Click **Export**. The Export Profile window appears (see Figure 4-6).

Figure 4-6 Export Profile Window



The profile name appears in the File name box.

Step 5 Choose a directory (such as your computer's floppy disk drive or a location on the network) from the Save in drop-down box.

Note The default location is the directory where ADU is installed (such as C:\Program Files\Cisco Aironet).

Step 6 Click **Save**. The profile is exported to the specified location.

Step 7 Follow the instructions in the "Importing a Profile" section to import the profile on another computer.

Configuring the Client Adapter

This chapter explains how to set the configuration parameters for a specific profile. The following topics are covered in this chapter:

- Overview, page 5-2
- Setting General Parameters, page 5-3
- Setting Advanced Parameters, page 5-6
- Setting Security Parameters, page 5-13
- Enabling Wi-Fi Multimedia, page 5-51
- Setting Roaming Parameters in the Windows Control Panel, page 5-55

Overview

When you choose to create a new profile or modify an existing profile on the Cisco Aironet Desktop Utility (Profile Management) window, the Profile Management windows appear. These windows enable you to set the configuration parameters for that profile.

Note If you do not change any of the configuration parameters for a newly created profile, the default values are used.

Note If you are planning to set parameters on more than one of the Profile Management windows, wait until you are finished with all of the windows before clicking **OK**. When you click **OK**, you are returned to the Cisco Aironet Desktop Utility (Profile Management) window.

Each of the Profile Management windows (listed below) contains parameters that affect a specific aspect of the client adapter:

- **General**—Prepares the client adapter for use in a wireless network
- **Advanced**—Controls how the client adapter operates within an infrastructure or ad hoc network
- **Security**—Controls how a client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data

Table 5-1 enables you to quickly locate instructions for setting each Profile Management window's parameters.

Table 5-1 Locating Configuration Instructions

Parameter Category	Page Number
General	5-3
Advanced	5-6
Security	5-13

Note If your system administrator used an administrative tool to deactivate certain parameters, these parameters are disabled on the Profile Management windows and cannot be selected.

Note You can also set two roaming parameters for your client adapter outside of ADU using the Windows Control Panel. Refer to the "Setting Roaming Parameters in the Windows Control Panel" section on page 5-55 for details.

Setting General Parameters

The Profile Management (General) window (see Figure 5-1) enables you to set parameters that prepare the client adapter for use in a wireless network. This window appears after you click **New** or **Modify** on the Cisco Aironet Desktop Utility (Profile Management) window.

Figure 5-1 Profile Management (General) Window

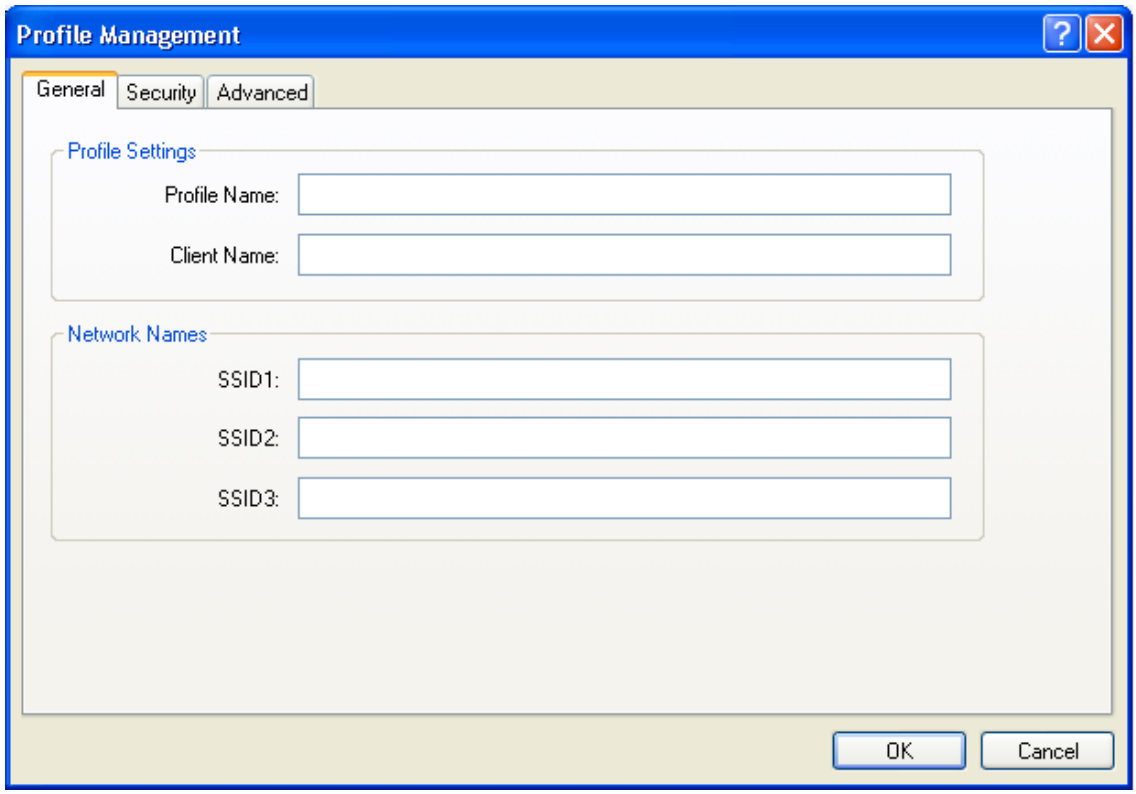


Table 5-2 lists and describes the client adapter's general parameters. Follow the instructions in the table to change any parameters.

Table 5-2 Profile Management General Parameters

Parameter	Description
Profile Name	The name assigned to the configuration profile. **Range:** You can key in up to 32 ASCII characters.
Client Name	A logical name for your workstation. It enables an administrator to ascertain which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point's list of connected devices. The client name is filled in automatically but can be changed. **Range:** You can key in up to 16 ASCII characters. **Default:** The name of your computer **Note** Each computer on the network should have a unique client name.
SSID1	The service set identifier (SSID) identifies the specific wireless network that you want the client adapter to access. **Range:** You can key in up to 32 ASCII characters (case sensitive). **Default:** A blank field **Note** If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs. If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter is unable to access the network. **Note** You must enter an SSID if this profile is configured for use in an ad hoc network.

Table 5-2 Profile Management General Parameters (continued)

Parameter	Description
SSID2	An optional SSID that identifies a second distinct network and enables the client adapter to roam to that network without having to be reconfigured. **Range:** You can key in up to 32 ASCII characters (case sensitive). **Default:** A blank field **Note** If a profile specifies more than one SSID, it cannot be included in auto profile selection. **Note** This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network.
SSID3	An optional SSID that identifies a third distinct network and enables the client adapter to roam to that network without having to be reconfigured. **Range:** You can key in up to 32 ASCII characters (case sensitive). **Default:** A blank field **Note** If a profile specifies more than one SSID, it cannot be included in auto profile selection. **Note** This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network.

Go to the next section to set additional parameters, or click **OK** to save your changes and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Setting Advanced Parameters

The Profile Management (Advanced) window (see Figure 5-2) enables you to set parameters that control how the client adapter operates within an infrastructure or ad hoc network. To open this window, click the **Advanced** tab from any Profile Management window.

Figure 5-2 Profile Management (Advanced) Window

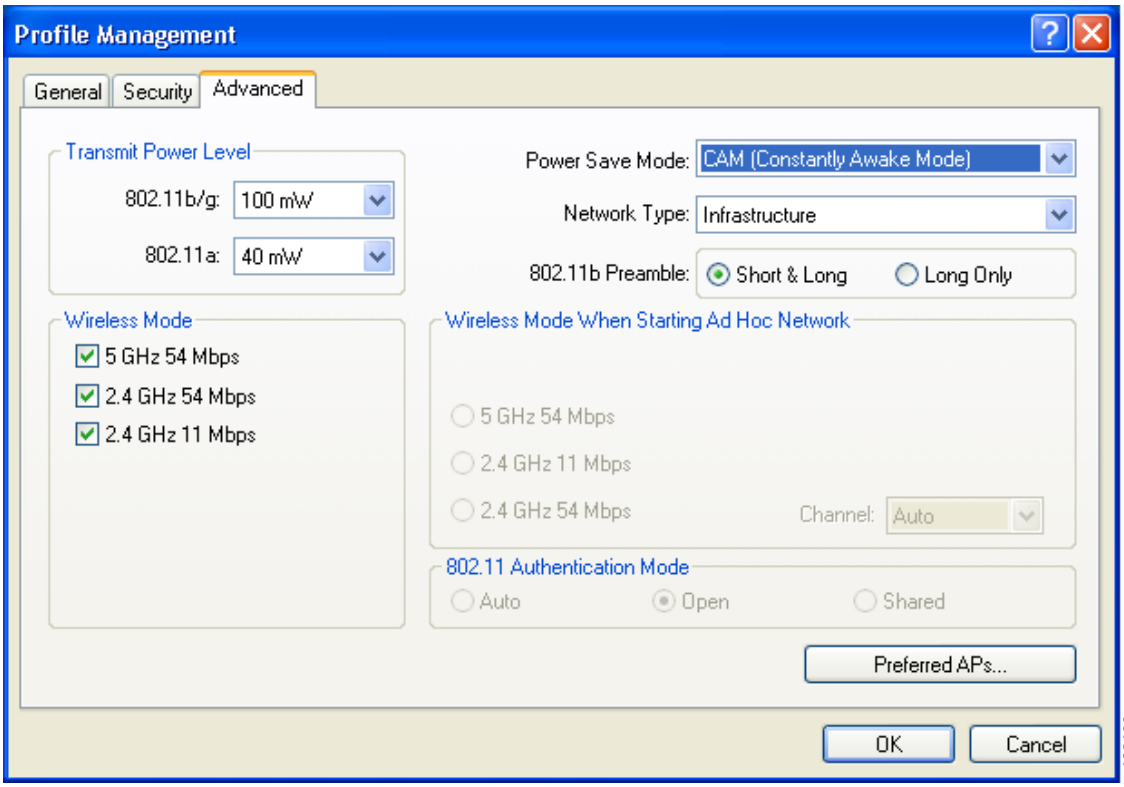


Table 5-3 lists and describes the client adapter's advanced parameters. Follow the instructions in the table to change any parameters.

Table 5-3 Profile Management Advanced Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Transmit Power Level</td><td>Specifies the preferred power level at which your client adapter transmits. Although the adapter supports up to 100 mW, the transmit power level that is actually used is limited to the maximum value allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, TELEC in Japan, etc.).

Options: Dependent on the radio band used and the power table programmed into the client adapter; see the table below.

Default: The maximum power level programmed into the client adapter and allowed by your country's regulatory agency

<table>
<tr><th>Radio Band</th><th>Transmit Power Level</th></tr>
<tr><td>802.11b/g</td><td>10, 20, 30, 50, 63, or 100 mW</td></tr>
<tr><td>802.11a</td><td>10, 13, 20, 25, or 40 mW</td></tr>
</table>
Note The client adapter's maximum transmit power level may be lower when operating in 802.11g mode than when operating in 802.11b mode due to 802.11g-specific regulatory limitations in some countries.

Note Reducing the transmit power level conserves battery power but decreases radio range.</td></tr>
</table>

Table 5-3 Profile Management Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Power Save Mode</td><td>Sets your client adapter to its optimum power consumption setting.

Options: CAM (Constantly Awake Mode), Fast PSP (Power Save Mode), or Max PSP (Max Power Saving)

Default: CAM (Constantly Awake Mode)

<table>
<tr><th>Power Save Mode</th><th>Description</th></tr>
<tr><td>CAM (Constantly Awake Mode)</td><td>Keeps the client adapter powered up continuously so there is little lag in message response time.

Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.</td></tr>
<tr><td>Fast PSP (Power Save Mode)</td><td>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.

Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</td></tr>
<tr><td>Max PSP (Max Power Saving)</td><td>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.

Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</td></tr>
</table>
Note If this profile is configured for use in an ad hoc network, CAM mode is used automatically.</td></tr>
</table>

Table 5-3 Profile Management Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Network Type</td><td>Specifies the type of network in which your client adapter is installed.
Options: Infrastructure or Ad Hoc
Default: Infrastructure

<table><tr><th>Network Type</th><th>Description</th></tr><tr><td>Ad Hoc</td><td>Often referred to as peer to peer. Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.</td></tr><tr><td>Infrastructure</td><td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td></tr></table></td></tr>
<tr><td>802.11b Preamble</td><td>Determines whether your client adapter uses both short and long radio headers or only long radio headers. The adapter can use short radio headers only if the access point is also configured to support them and is using them. If any clients associated to an access point are using long headers, then all clients in that cell must use long headers, even if both this client and the access point have short radio headers enabled.
Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers.
Options: Short & Long or Long Only
Default: Short & Long
Note This parameter is disabled if the Wireless Mode parameter is set to 5 GHz 54 Mbps only.</td></tr>
</table>

Table 5-3 Profile Management Advanced Parameters (continued)

Parameter	Description
Wireless Mode	Specifies the frequency and rate at which your client adapter should transmit packets to or receive packets from access points. **Options:** 5 GHz 54 Mbps, 2.4 GHz 54 Mbps, and 2.4 GHz 11 Mbps **Default:** All options selected **Note** When more than one option is selected, the client adapter attempts to use the wireless modes in this order: 5 GHz 54 Mbps, 2.4 GHz 54 Mbps, 2.4 GHz 11 Mbps. **Note** If you choose 2.4 GHz 11 Mbps, the client adapter can associate to access points containing an 802.11b or 802.11g radio at 802.11b data rates. If you choose 2.4 GHz 54 Mbps, the client adapter can associate to access points containing an 802.11b radio at 802.11b data rates or to access points containing an 802.11g radio at 802.11b or 802.11g data rates. **Note** When you enable auto profile selection, the client adapter ignores the selected profile's wireless mode setting and scans all wireless modes for an available network. Using this method, the client does not need to drop the current connection nor change the current profile while looking for networks in other profiles. **Note** Your client adapter's wireless mode must match that of the access points with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.
Wireless Mode When Starting Ad Hoc Network	Specifies the frequency and rate at which your client adapter should transmit packets to or receive packets from other clients (in ad hoc mode). **Options:** 5 GHz 54 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps **Default:** 5 GHz 54 Mbps **Note** The client scans the band(s) specified by the Wireless Mode parameter before creating a new ad hoc cell based on the band specified by the Wireless Mode When Starting Ad Hoc Network parameter. **Note** Your client adapter's wireless mode must match that of the other clients with which it is to communicate. Otherwise, your client adapter may not be able to associate to them. **Note** The 2.4 GHz 54 Mbps wireless mode may not be functional on some vendors' products. In this case, the client adapter uses the 2.4 GHz 11 Mbps wireless mode.

Table 5-3 Profile Management Advanced Parameters (continued)

Parameter	Description
Channel	Specifies the channel that your client adapter uses for communications in a 2.4-GHz ad hoc network. The available channels conform to the IEEE 802.11 Standard for your regulatory domain. The channel of the client adapter must be set to match the channel used by the other clients in the wireless network. If the client adapter does not find any other ad hoc clients, this parameter specifies the channel with which the adapter will start its cell. **Range:** Dependent on regulatory domain **Example:** 1 to 11 (2412 to 2462 MHz) in North America **Default:** Auto (the client automatically determines the channel on which to start communications) **Note** This parameter is available only when 2.4 GHz 11 Mbps is selected for the Wireless Mode When Starting Ad Hoc Network parameter. When 5 GHz 54 Mbps is selected, the Channel parameter is set to Auto automatically. **Note** Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

Table 5-3 Profile Management Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>802.11 Authentication Mode</td><td>Specifies how your client adapter attempts to authenticate to an access point. Open and shared authentication do not rely on a RADIUS server on your network.

Options: Auto, Open, or Shared

Default: Open

<table>
<tr><th>802.11 Authentication Mode</th><th>Description</th></tr>
<tr><td>Auto</td><td>Causes the client adapter to attempt to authenticate using shared authentication. If it fails, the client adapter then attempts to authenticate using open authentication.</td></tr>
<tr><td>Open</td><td>Enables your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. However, communication can occur only if the adapter’s WEP key matches that of the access point.</td></tr>
<tr><td>Shared</td><td>Enables your client adapter to authenticate and communicate only with access points that have the same WEP key.

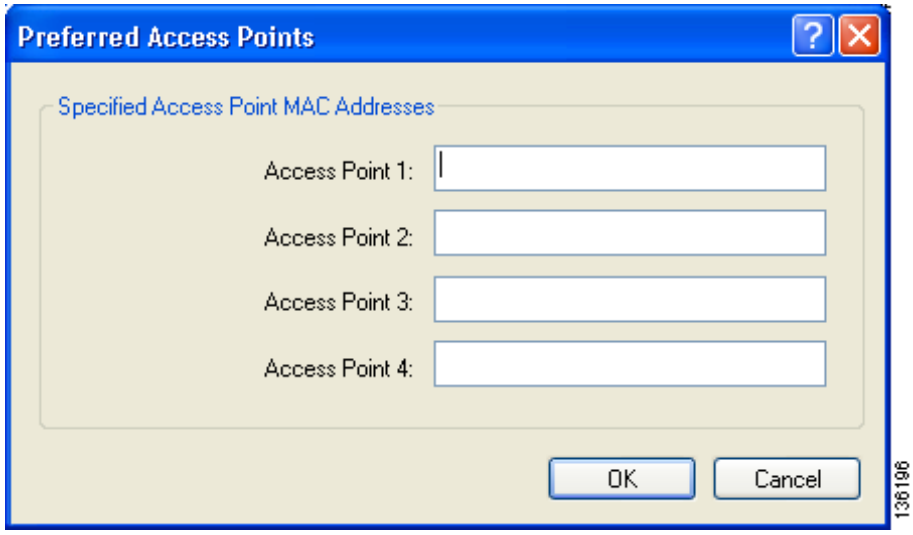
During shared key authentication, the access point sends an unencrypted challenge packet to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter. If the packet is successfully encrypted/ decrypted, the user is considered to be authenticated.</td></tr>
</table>
Note Cisco recommends that Auto and Shared not be used because they present a security risk.

Note Your client adapter’s 802.11 authentication mode setting must match that of the access points with which it is to communicate. Otherwise, your client adapter may not be able to authenticate to them.

Note If this profile is configured for use in an ad hoc network or is not configured to use static WEP, this parameter is unavailable, and Open authentication is used.</td></tr>
</table>

If this profile is configured for use in an infrastructure network and you want to specify up to four access points to which the client adapter should attempt to associate, click **Preferred APs**. The Preferred Access Points window appears (see Figure 5-3).

Figure 5-3 Preferred Access Points Window



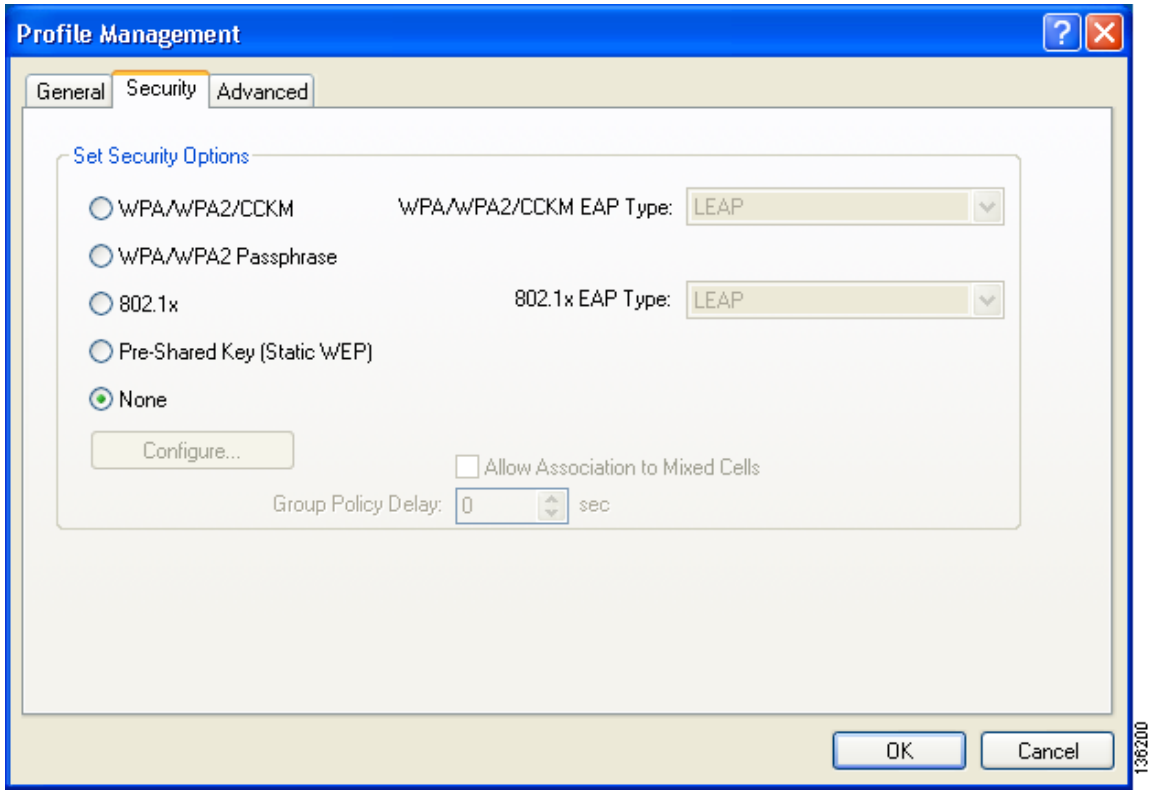
Leave the Access Point 1 through Access Point 4 fields blank or enter the MAC addresses of up to four preferred access points to which the client adapter can associate; then click **OK**. (The MAC address should consist of 12 hexadecimal characters.) If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point.

Go to the next section to set additional parameters or click **OK** to save your changes and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Setting Security Parameters

The Profile Management (Security) window (see Figure 5-4) enables you to set parameters that control how the client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data. To access this window, click the **Security** tab from any Profile Management window.

Figure 5-4 Profile Management (Security) Window



This window is different from the other Profile Management windows in that it includes many security features, each of which involves a number of steps. In addition, the security features themselves are complex and need to be understood before they are implemented. Therefore, this section provides an overview of the security features as well as procedures for enabling them.

Overview of Security Features

You can protect your data as it is transmitted through your wireless network by encrypting it through the use of wired equivalent privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the EAP authentication process. The information in the "Static WEP Keys" and "EAP (with Dynamic WEP Keys)" sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

WEP keys, whether static or dynamic, are either 40 or 128 bits in length. 128-bit WEP keys offer a greater level of security than 40-bit WEP keys.

Note Refer to the "Additional WEP Key Security Features" section on page 5-20 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

Each device (or profile) within your wireless network can be assigned up to four static WEP keys. If a device receives a packet that is not encrypted with the appropriate key (as the WEP keys of all devices that are to communicate with each other must match), the device discards the packet and never delivers it to the intended receiver.

You do not need to re-enter static WEP keys each time the client adapter is inserted or the Windows device is rebooted because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter's registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

The Define Pre-Shared Keys window enables you to view the WEP key settings for a particular profile and to assign new WEP keys or overwrite existing WEP keys. Refer to the "Enabling Static WEP" section on page 5-24 for instructions.

EAP (with Dynamic WEP Keys)

The standard for wireless LAN security, as defined by IEEE, is called *802.1X for 802.11*, or simply *802.1X*. An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network.

Five 802.1X authentication types are available in ADU for use with Windows 2000 or XP:

- **EAP-Cisco Wireless** (or **LEAP**)—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. ADU offers a variety of LEAP configuration options, including how a username and password are entered to begin the authentication process.

  The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The username and password need to be re-entered each time the client adapter is inserted or the Windows device is rebooted unless you configure your adapter to use saved LEAP credentials.

  RADIUS servers that support LEAP include Cisco Secure ACS release 2.6 or later, Cisco Access Registrar release 1.7 or later, Funk Software's Steel-Belted RADIUS release 4.1 or later, and Meetinghouse Data Communications' AEGIS release 1.1 or later.

- **EAP-FAST**—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunneled authentication process to provide advanced 802.1X EAP mutual authentication.

  – Phase 0 enables the client to dynamically provision a protected access credentials (PAC) when necessary. During this phase, a PAC is generated securely between the user and the network.

  – Phase 1 uses the PAC to establish a mutually authenticated and secure tunnel between the client and the RADIUS server. RADIUS servers that support EAP-FAST include Cisco Secure ACS version 3.2.3 and later.

  – Phase 2 performs client authentication in the established tunnel.

  ADU offers a variety of EAP-FAST configuration options, including how and when a username and password are entered to begin the authentication process and whether automatic or manual PAC provisioning is used.

The client adapter uses the username, password, and PAC to perform mutual authentication with the RADIUS server through the access point. The username and password need to be re-entered each time the client adapter is inserted or the Windows device is rebooted unless you configure your adapter to use saved EAP-FAST credentials.

PACs are created by Cisco Secure ACS and are identified by an ID. The user obtains his or her own copy of the PAC from the server, and the ID links the PAC to the profile created in ADU. When manual PAC provisioning is enabled, the PAC is manually copied from the server and imported onto the client device. The following rules govern PAC storage:

- PACs are stored as encrypted data files in either the global or private store on the user's computer.
  - Global PACs can be accessed and used by any user at any logon stage. They are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User Is Logged In option.
  - Private PACs can be accessed and used only by the user who provisioned them or the system administrator.

Note Global PACs are stored on C:\Document and Settings\All Users\Application Data\Cisco\cscostore, and private PACs are stored on C:\Document and Settings*user*\Application Data\Cisco\cscostore.

- If automatic PAC provisioning is enabled and it occurs after the user is logged on, the PAC is stored in the private store of the currently logged-on user. Otherwise, the PAC is stored in the global store.
- PAC files can be added or overwritten using the import feature.
- PAC files can be removed using the delete feature. They are also deleted when you uninstall the client adapter software.

EAP-FAST authentication is designed to support the following user databases over a wireless LAN:

- Cisco Secure ACS internal user database
- Cisco Secure ACS ODBC user database
- Windows NT/2000/2003 domain user database
- LDAP user database

LDAP user databases (such as NDS) support only manual PAC provisioning while the other three user databases support both automatic and manual PAC provisioning.

- **EAP-TLS**—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.

  RADIUS servers that support EAP-TLS include Cisco Secure ACS release 3.0 or later and Cisco Access Registrar release 1.8 or later.

- **PEAP (EAP-GTC)**—This PEAP authentication type is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP (EAP-GTC) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. If your network uses an OTP user database, PEAP (EAP-GTC) requires you to enter a hardware or software token password to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (EAP-GTC) requires you to enter your username, password, and domain name in order to start the authentication process.

  RADIUS servers that support PEAP (EAP-GTC) authentication include Cisco Secure ACS release 3.1 or later.

- **PEAP (EAP-MSCHAP V2)**—This PEAP authentication type is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

  RADIUS servers that support PEAP (EAP-MSCHAP V2) authentication include Cisco Secure ACS release 3.2 or later.

When you configure your access point as indicated in Table 5-4 on page 5-20 and configure your client adapter for LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), authentication to the network occurs in the following sequence:

1. The client associates to an access point and begins the authentication process.

   Note The client does not gain full access to the network until authentication between the client and the RADIUS server is successful.

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (LEAP and PEAP), password and PAC (EAP-FAST), or certificate (EAP-TLS) being the shared secret for authentication. The password and PAC are never transmitted during the process.
3. If authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.
4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.
5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets (and broadcast packets if the access point is set up to do so) that travel between them.

Refer to the following pages for instructions on enabling these EAP types:

- LEAP, page 5-27
- EAP-FAST, page 5-31
- EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), page 5-39

Note Refer to the IEEE 802.11 Standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ab.html

WPA and WPA2

Wi-Fi Protected Access (WPA) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

WPA uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA and WPA2 use 802.1X for authenticated key management.

Both WPA and WPA2 support two mutually exclusive key management types: WPA/WPA2 and WPA/WPA2 passphrase (also known as *WPA pre-shared key* or *WPA-PSK*). Using WPA or WPA2, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). The server generates the PMK dynamically and passes it to the access point. Using WPA or WPA2 passphrase, however, you configure a passphrase (or pre-shared key) on both the client and the access point, and that passphrase is used as the PMK.

Refer to the following pages for instructions on enabling these WPA variations:

- WPA/WPA2 Passphrase, page 5-26
- LEAP with WPA/WPA2, page 5-27
- EAP-FAST with WPA/WPA2, page 5-31
- EAP-TLS with WPA/WPA2, page 5-40
- PEAP (EAP-GTC) with WPA/WPA2, page 5-42
- PEAP (EAP-MSCHAP V2) with WPA/WPA2, page 5-46

Note WPA must also be enabled on the access point. To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. Refer to the documentation for your access point for instructions on enabling this feature.

CCKM Fast Secure Roaming

Some applications that run on a client device may require fast roaming between access points. Voice applications, for example, require it to prevent delays and gaps in conversation. CCKM fast secure roaming is enabled automatically in Install Wizard 1.0 or later for LEAP-enabled CB21AG and PI21AG clients using WPA/WPA2 and in Install Wizard 2.0 or later for CB21AG and PI21AG clients using WPA/WPA2/CCKM with EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2). However, this feature must be enabled on the access point.

During normal operation, EAP-enabled clients mutually authenticate with a new access point by performing a complete EAP authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for CCKM fast secure roaming, EAP-enabled clients securely roam from one access point to another without the need to reauthenticate with the RADIUS server. Using Cisco Centralized Key Management (CCKM), an access point that is configured for wireless domain services (WDS) uses a fast rekeying technique that enables Cisco client devices to roam from one access point to another typically in under 150 milliseconds (ms). CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions.

Note If you want to enable CCKM fast secure roaming on the client adapter, you must choose the WPA/WPA2/CCKM security option on the Profile Management (Security) window, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Access points must use Cisco IOS Release 12.2(11)JA or later to enable CCKM fast secure roaming. Refer to the documentation for your access point for instructions on enabling this feature.

Note The Microsoft Wireless Configuration Manager and the Microsoft 802.1X supplicant, if installed, must be disabled in order for CCKM fast secure roaming to operate correctly. If your computer is running Windows XP and you chose to configure your client adapter using ADU during installation, these features should already be disabled. Similarly, if your computer is running Windows 2000, the Microsoft 802.1X supplicant, if installed, should already be disabled. Refer to Chapter 10 if you need additional information.

Reporting Access Points that Fail LEAP Authentication

The CB21AG and PI21AG client adapters and the following access point firmware versions support a feature that is designed to detect access points that fail LEAP authentication:

- 12.00T or later (access points running VxWorks)
- Cisco IOS Release 12.2(4)JA or later (1100 series access points)
- Cisco IOS Release 12.2(8)JA or later (1200 series access points)
- Cisco IOS Release 12.2(13)JA or later (350 series access points)

An access point running one of these firmware versions records a message in the system log when the client discovers and reports another access point in the wireless network that has failed LEAP authentication.

The process takes place as follows:

1. A client with a LEAP profile attempts to associate to access point A.
2. Access point A does not handle LEAP authentication successfully, perhaps because the access point does not understand LEAP or cannot communicate to a trusted LEAP authentication server.
3. The client records the MAC address for access point A and the reason why the association failed.
4. The client associates successfully to access point B.
5. The client sends the MAC address of access point A and the reason code for the failure to access point B.
6. Access point B logs the failure in the system log.

Note This feature does not need to be enabled on the client adapter or access point; it is supported automatically by both devices. However, the access points must use the specified firmware versions or later.

Additional WEP Key Security Features

The three security features discussed in this section (MIC, TKIP, and broadcast key rotation) are designed to prevent sophisticated attacks on your wireless network's WEP keys. These features do not need to be enabled on the client adapter; they are supported automatically in the client adapter software. However, they must be enabled on the access point.

Note Refer to the documentation for your access point for instructions on enabling these security features.

Message Integrity Check (MIC)

MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC adds a few bytes to each packet to make the packets tamper-proof.

The Advanced Status window indicates if MIC is being used, and the Advanced Statistics window provides MIC statistics.

Temporal Key Integrity Protocol (TKIP)

This feature, also referred to as *WEP key hashing*, defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. It protects both unicast and broadcast WEP keys.

Note TKIP is enabled automatically when WPA is enabled, and it is disabled when WPA is disabled.

Broadcast Key Rotation

When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select.

Synchronizing Security Features

In order to use any of the security features discussed in this section, both your client adapter and the access point to which it will associate must be set appropriately. Table 5-4 indicates the client and access point settings required for each security feature. This chapter provides specific instructions for enabling the security features on your client adapter. Refer to the documentation for your access point for instructions on enabling any of these features on the access point.

Table 5-4 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Choose Open authentication and Pre-Shared Key (Static WEP) and create a WEP key	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Choose Shared authentication and Pre-Shared Key (Static WEP) and create a WEP key	Set up and enable WEP and enable Shared Key Authentication for the SSID

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
WPA or WPA2 passphrase (or WPA or WPA2 pre-shared key)	Choose WPA/WPA2 Passphrase and enter the passphrase	Choose a cipher suite, enable Open Authentication and WPA for the SSID, and enter a WPA pre-shared key **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
LEAP authentication	Choose 802.1x and LEAP; then set LEAP settings	Set up and enable WEP and enable Network-EAP Authentication for the SSID
LEAP authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and LEAP; then set LEAP settings	For WPA, choose a cipher suite that includes TKIP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID For WPA2, choose a cipher suite that includes AES-CCMP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
EAP-FAST authentication	Choose 802.1x and EAP-FAST, set EAP-FAST settings, and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable both Network-EAP and Open with EAP Authentication for the SSID
EAP-FAST authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and EAP-FAST, set EAP-FAST settings, and enable automatic provisioning or import a PAC file	For WPA, choose a cipher suite that includes TKIP and enable both Network-EAP and Open with EAP Authentication as well as WPA for the SSID For WPA2, choose a cipher suite that includes AES-CCMP and enable both Network-EAP and Open with EAP Authentication as well as WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-TLS authentication		
If using ADU to configure card	Choose 802.1x and EAP-TLS; then set EAP-TLS settings	Set up and enable WEP and enable Open with EAP Authentication for the SSID
If using Windows XP to configure card	Choose Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable Open with EAP Authentication for the SSID
EAP-TLS authentication with WPA or WPA2		
If using ADU to configure card	Choose WPA/WPA2/CCKM and EAP-TLS; then set EAP-TLS settings	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
If using Windows XP to configure card	Enable WPA and choose Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type **Note** WPA2 is not yet available in the Microsoft Wireless Configuration Manager in Windows XP.	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
PEAP authentication		
If using ADU to configure card	Choose 802.1x and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	Set up and enable WEP and enable Open with EAP Authentication for the SSID
If using Windows XP to configure card	Choose Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Open with EAP Authentication for the SSID

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
PEAP authentication with WPA or WPA2		
If using ADU to configure card	Choose WPA/WPA2/CCKM and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
If using Windows XP to configure card	Enable WPA and choose Enable network access control using IEEE 802.1X and PEAP as the EAP Type **Note** WPA2 is not yet available in the Microsoft Wireless Configuration Manager in Windows XP.	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
CCKM fast secure roaming	Choose WPA/WPA2/CCKM and LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP MSCHAP V2); then set the EAP authentication settings **Note** If you want to enable CCKM, you must choose WPA/WPA2/CCKM, regardless of whether you want the client adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.	Use Cisco IOS Release 12.2(11)JA or later, choose a cipher suite that is compatible with CCKM, enable both Network-EAP and Open with EAP Authentication and CCKM for the SSID, and configure for participation in wireless domain services (WDS) **Note** To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.
Reporting access points that fail LEAP authentication	No settings required; automatically enabled	No settings required; automatically enabled in the firmware versions listed on page 5-19.
MIC	No settings required; automatically enabled	Set up and enable WEP with full encryption, set MIC to MMH or check the Enable MIC check box, and set Use Aironet Extensions to Yes

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
TKIP	No settings required; automatically enabled	Set up and enable WEP, set TKIP to Cisco or check the Enable Per Packet Keying check box, and set Use Aironet Extensions to Yes
Broadcast key rotation	Enable LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2)	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

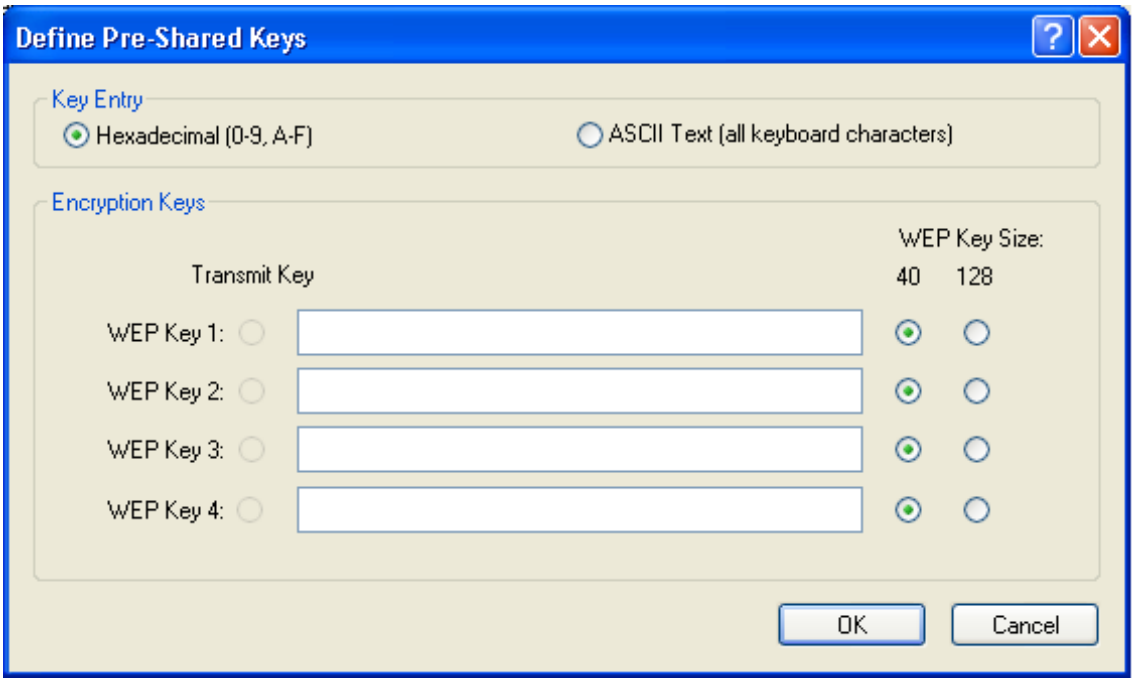
Enabling Static WEP

Follow the steps below to enable static WEP for this profile.

Step 1 Choose **Pre-Shared Key (Static WEP)** on the Profile Management (Security) window.

Step 2 Click **Configure**. The Define Pre-Shared Keys window appears (see Figure 5-5).

Figure 5-5 Define Pre-Shared Keys Window



Step 3 Choose one of the following WEP key entry methods:

- **Hexadecimal (0-9, A-F)**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text (all keyboard characters)**—Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.

Note ASCII text WEP keys are not supported on the Cisco Aironet 1200 Series Access Points, so you must choose the Hexadecimal (0-9, A-F) option if you are planning to use your client adapter with these access points.

Step 4 For the static WEP key that you are entering (1, 2, 3, or 4), choose a WEP key size of 40 or 128 on the right side of the window. 128-bit client adapters can use 40- or 128-bit keys, but 40-bit adapters can use only 40-bit keys. If 128 bit is not supported by the client adapter, this option is unavailable.

Step 5 Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:

- WEP keys must contain the following number of characters:
  - 10 hexadecimal characters or 5 ASCII text characters for 40-bit keys

    Example: 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
  - 26 hexadecimal characters or 13 ASCII text characters for 128-bit keys

    Example: 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)

Note You must enter hexadecimal characters if your client adapter will be used with Cisco Aironet 1200 Series Access Points.

- Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
- When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.

Note All existing static WEP keys are displayed as bullets for security reasons. If you need to modify a WEP key, simply click in the WEP key field, delete the bullets, and enter a new key.

Step 6 Click the **Transmit Key** button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.

Step 7 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 8 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 9 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Enabling WPA/WPA2 Passphrase

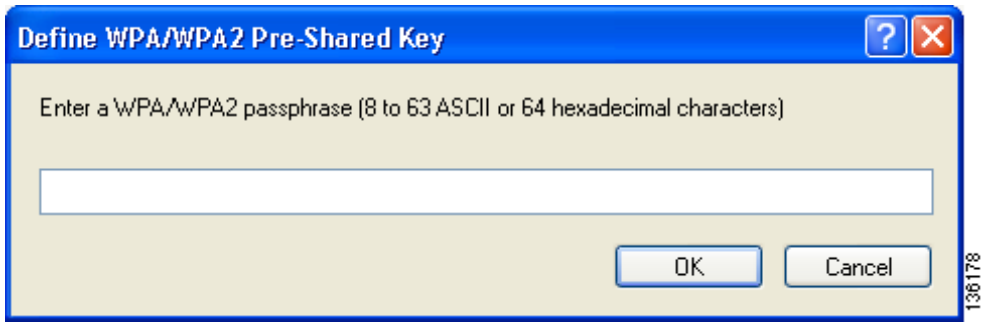
Follow the steps below to enable WPA/WPA2 passphrase (also known as *WPA/WPA2 pre-shared key*) for this profile.

Note To use WPA passphrase, client adapters must use the software included in Install Wizard 1.0 or later and access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2 passphrase, client adapters must use the software included in Install Wizard 2.0 or later and access points must use Cisco IOS Release 12.3(2)JA or later.

Step 1 Choose **WPA/WPA2 Passphrase** on the Profile Management (Security) window.

Step 2 Click **Configure**. The Define WPA/WPA2 Pre-Shared Key window appears (see Figure 5-6).

Figure 5-6 Define WPA/WPA2 Pre-Shared Key Window



Step 3 Obtain the WPA/WPA2 passphrase for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in the WPA/WPA2 passphrase field. Follow the guidelines below to enter a passphrase:

- WPA/WPA2 passphrases must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- Your client adapter's WPA/WPA2 passphrase must match the passphrase used by the access point with which you are planning to communicate.

Step 4 Click **OK** to save the passphrase and return to the Profile Management (Security) window.

Step 5 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 6 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Enabling LEAP

Before you can enable LEAP authentication, your network devices must meet the following requirements:

- To use LEAP authentication with WPA2, client adapters must use the software included in Install Wizard 2.0 or later.
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (access points running VxWorks), Cisco IOS Release 12.2(4)JA (1100 series access points), Cisco IOS Release 12.2(8)JA (1200 series access points), or Cisco IOS Release 12.2(13)JA (350 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. To use the Reporting Access Points That Fail LEAP Authentication feature, access points must use the firmware versions listed on page 5-20.

- All necessary infrastructure devices (such as access points, servers, etc.) must be properly configured for LEAP authentication.

Follow the steps below to enable LEAP authentication for this profile.

Step 1 Perform one of the following on the Profile Management (Security) window:

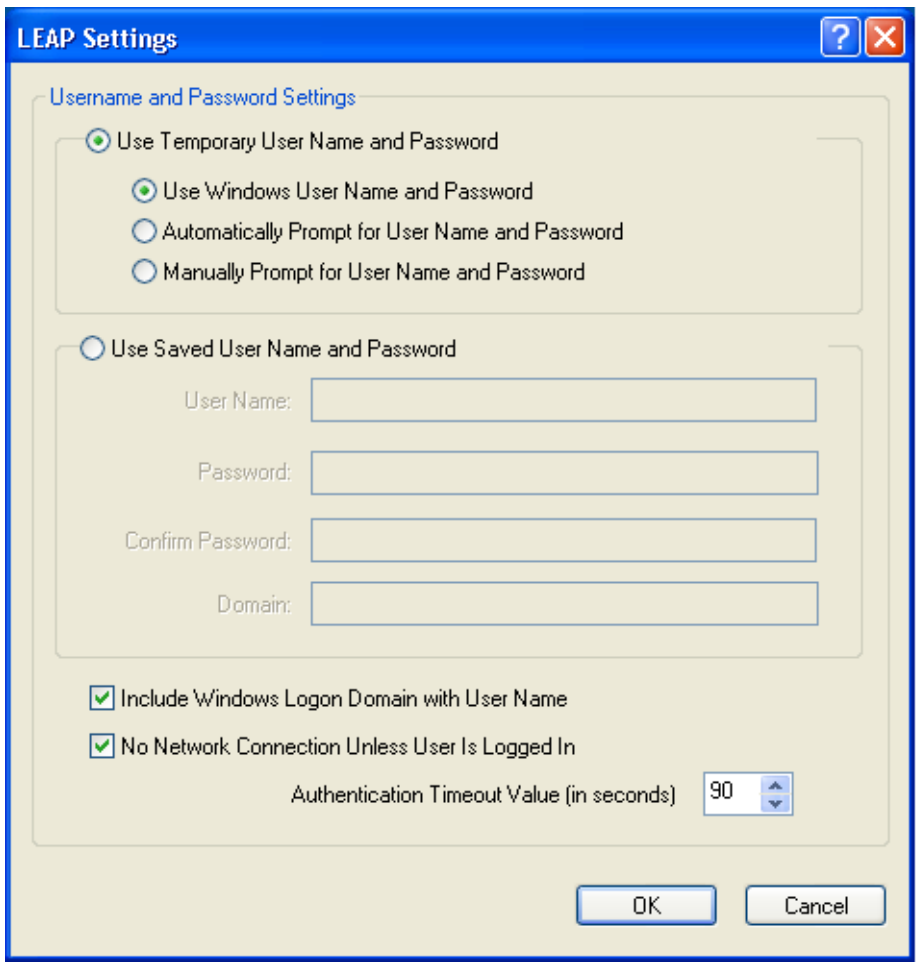
- If you want to enable LEAP without WPA or WPA2, choose **802.1x** under Set Security Options and **LEAP** in the 802.1x EAP Type drop-down box.
- If you want to enable LEAP with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **LEAP** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-18 for additional information.

Step 2 Click **Configure**. The LEAP Settings window appears (see Figure 5-7).

Figure 5-7 LEAP Settings Window



Step 3 Choose one of the following LEAP username and password setting options:

- **Use Temporary User Name and Password**—Requires you to enter the LEAP username and password each time the computer reboots in order to authenticate and gain access to the network.
- **Use Saved User Name and Password**—Does not require you to enter a LEAP username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

Step 4 Perform one of the following:

- If you chose Use Temporary User Name and Password in Step 3, choose one of the following options:
  - **Use Windows User Name and Password—**Causes your Windows username and password to also serve as your LEAP username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for User Name and Password**—Requires you to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for User Name and Password**—Requires you to manually invoke the LEAP authentication process as needed using the Manual Login option in the Action drop-down menu or ASTU. You are not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- If you chose Use Saved User Name and Password in Step 3, follow these steps:
  a. Enter a username and password in the appropriate fields.
  b. Re-enter the password in the Confirm Password field.
  c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.

Step 5 If you work in an environment with multiple domains and therefore want your Windows login domain to be passed to the RADIUS server along with your username, check the **Include Windows Logon Domain with User Name** check box. The default setting is checked.

Note If you chose to use a saved username and password but do not check the Include Windows Logon Domain with User Name check box, the saved domain name is not passed to the RADIUS server.

Step 6 If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection Unless User Is Logged In** check box. The default setting is checked.

Step 7 In the Authentication Timeout Value field, choose the amount of time (in seconds) before a LEAP authentication attempt is considered to be failed and an error message appears.

Range: 30 to 500 seconds

Default: 90 seconds

Step 8 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 9 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 10 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 11 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 12 Refer to Chapter 6 for instructions on authenticating using LEAP.

Enabling EAP-FAST

Before you can enable EAP-FAST authentication, your network devices must meet the following requirements:

- To use EAP-FAST authentication with WPA2, client adapters must use the software included in Install Wizard 2.0 or later.
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 11.54T (1200 series access points), or Cisco IOS Release 12.2(4)JA (1100 series access points).

Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication feature, access points must use the firmware versions listed on page 5-19.

Note The access point to which your client adapter will associate must be configured for both Network-EAP and Open authentication.

- All necessary infrastructure devices (such as access points, servers, gateways and user databases) must be properly configured for EAP-FAST authentication.

Follow these steps to enable EAP-FAST authentication for this profile.

Step 1 Perform one of the following on the Profile Management (Security) window:

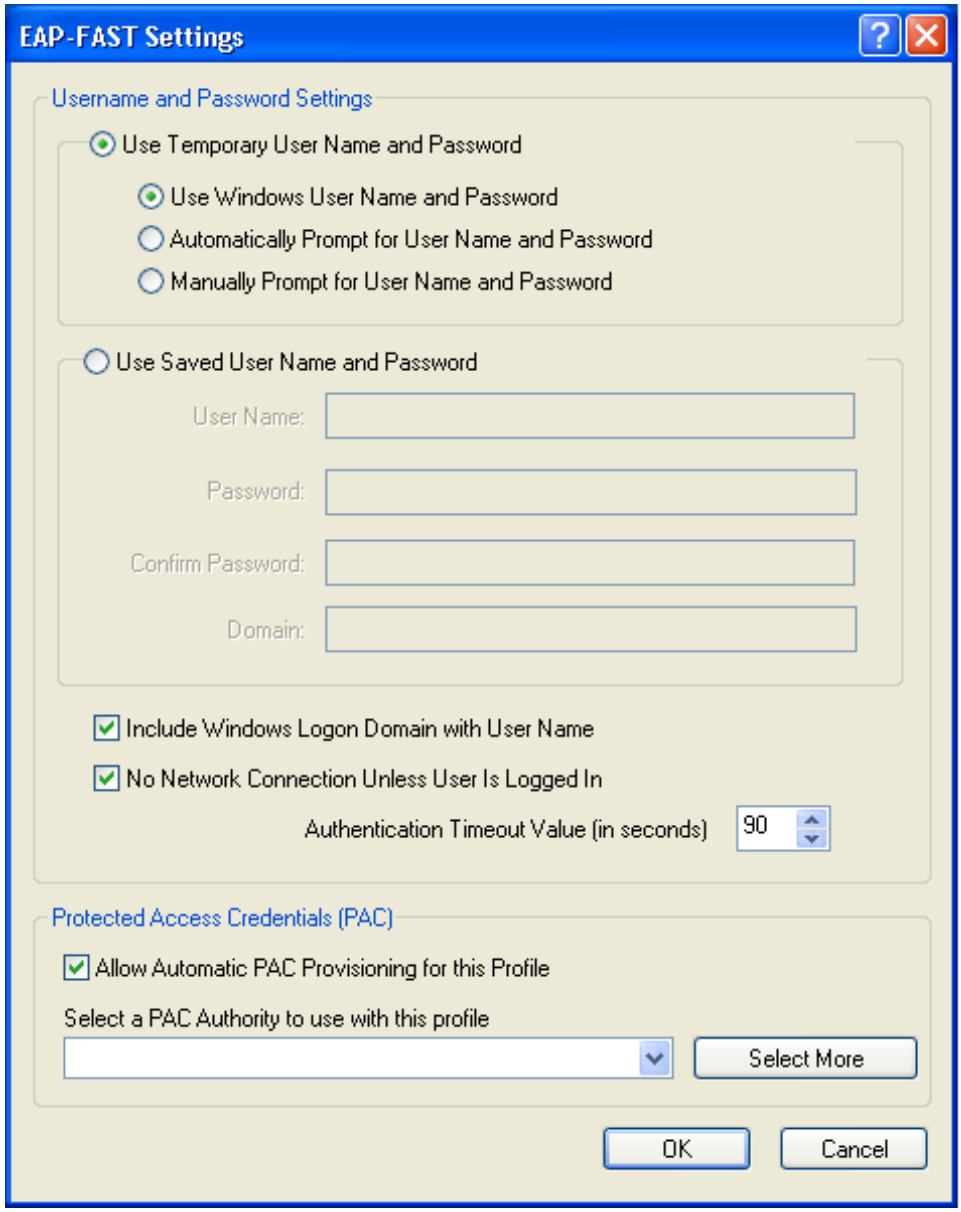
- If you want to enable EAP-FAST without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-FAST** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-FAST with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-FAST** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-18 for additional information.

Step 2 Click **Configure**. The EAP-FAST Settings window appears (see Figure 5-8).

Figure 5-8 EAP-FAST Settings Window



Step 3 Choose one of the following EAP-FAST username and password setting options:

- **Use Temporary User Name and Password**—Requires you to enter the EAP-FAST username and password each time the computer reboots in order to authenticate and gain access to the network.
- **Use Saved User Name and Password**—Does not require you to enter an EAP-FAST username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

Step 4 Perform one of the following:

- If you chose Use Temporary User Name and Password in Step 3, choose one of the following options:
  - **Use Windows User Name and Password—**Causes your Windows username and password to also serve as your EAP-FAST username and password, giving you only one set of credentials to remember. After you log in, the authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for User Name and Password**—Requires you to enter a separate EAP-FAST username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the authentication process.
  - **Manually Prompt for User Name and Password**—Requires you to manually invoke the EAP-FAST authentication process as needed using the Manual Login option in the Action drop-down menu or ASTU. You are not prompted to enter an EAP-FAST username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- If you chose Use Saved User Name and Password in Step 3, follow these steps:
  a. Enter a username and password in the appropriate fields.
  b. Re-enter the password in the Confirm Password field.
  c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.

Step 5 If you work in an environment with multiple domains and therefore want your Windows login domain to be passed to the RADIUS server along with your username, check the **Include Windows Logon Domain with User Name** check box. The default setting is checked.

Note If you chose to use a saved username and password but do not check the Include Windows Logon Domain with User Name check box, the saved domain name is not passed to the RADIUS server.

Step 6 If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection Unless User Is Logged In** check box. The default setting is checked.

Step 7 In the Authentication Timeout Value field, choose the amount of time (in seconds) before an EAP-FAST authentication attempt is considered to be failed and an error message appears.

Range: 30 to 500 seconds

Default: 90 seconds

Step 8 Perform one of the following:

- If you want to enable automatic PAC provisioning, make sure the **Allow Automatic PAC Provisioning for this Profile** check box is checked. A protected access credentials (PAC) is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.). This is the default setting.
- If you want to enable manual PAC provisioning, uncheck the **Allow Automatic PAC Provisioning for this Profile** check box. This option requires you to choose a PAC authority or manually import a PAC file.

Note LDAP user databases support only manual PAC provisioning while Cisco Secure ACS internal, Cisco Secure ODBC, and Windows NT/2000/2003 domain user databases support both automatic and manual PAC provisioning.

Note Provisioning occurs only upon initial negotiation of the PAC or upon PAC expiration. After the PAC is provisioned, it serves as the per-user key by which authentication transactions are secured.

Step 9 From the Select a PAC Authority To Use with This Profile drop-down box, highlight the PAC authority that is associated with the network defined by the profile's SSID. The list contains the names of all the authentication servers from which you have previously provisioned a PAC.

If the PAC authority drop-down box is empty or does not contain the name of a desired PAC authority, go to Step 10 to import a PAC file.

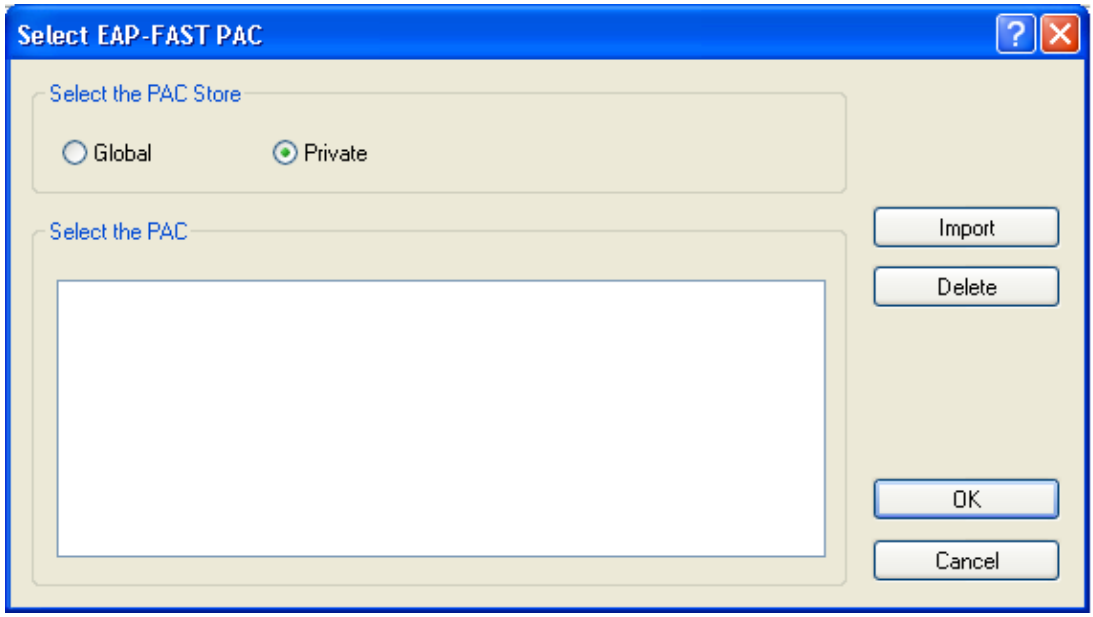
Note This step is required for manual PAC provisioning but optional for automatic PAC provisioning. If automatic provisioning is enabled, automatic provisioning will be initiated during the authentication process of the EAP-FAST profile if no PAC authority was selected, the PAC could not be found, or the specified PAC does not match the server ID.

Note If you have multiple PACs for a given PAC authority, you can select a specific PAC from those that have already been imported or auto-provisioned by following these steps:
a. Click **Select More**.
b. Choose the PAC store from which you want to select a PAC file.
c. Select the desired PAC from the Select the PAC list on the Select EAP-FAST PAC window.
d. Click **OK**.
e. Go to Step 11.

Step 10 If necessary, follow these steps to import a PAC file:

a. Click **Select More**. The Select EAP-FAST PAC window appears (see Figure 5-9).

Figure 5-9 Select EAP-FAST PAC Window

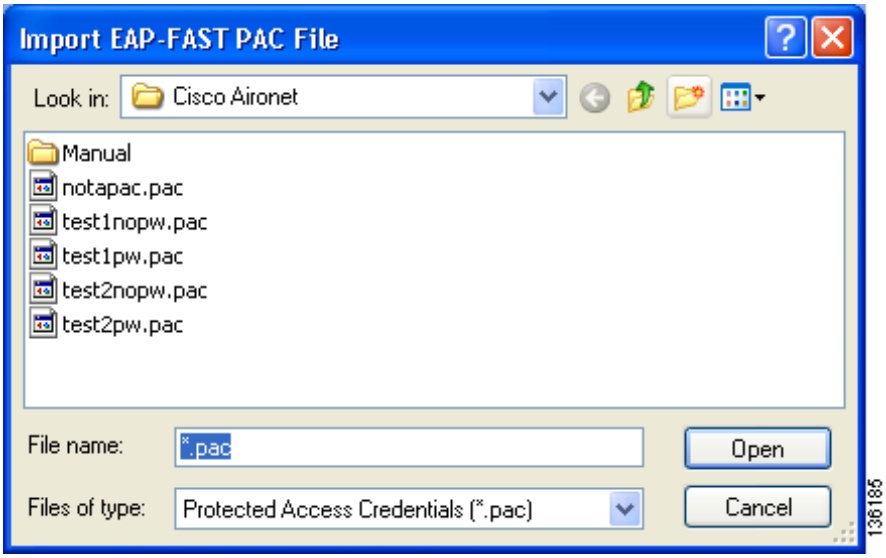


b. Choose one of these PAC store options to determine where the imported PAC file will be stored and to whom it will be accessible:

- **Global**—PACs that are stored in the global PAC store can be accessed and used by any user at any logon stage. Global PACs are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User Is Logged In option.
- **Private**—PACs that are stored in the private store can be accessed and used only by the user who provisioned them or the system administrator. They are not accessible until the user is logged onto the local system. This is the default option.

c. Click **Import**. The Import EAP-FAST PAC File window appears (see Figure 5-10).

Figure 5-10 Import EAP-FAST PAC File Window



d. Find the location of the PAC file in the Look in box. The default location is C:\Program Files\Cisco Aironet.

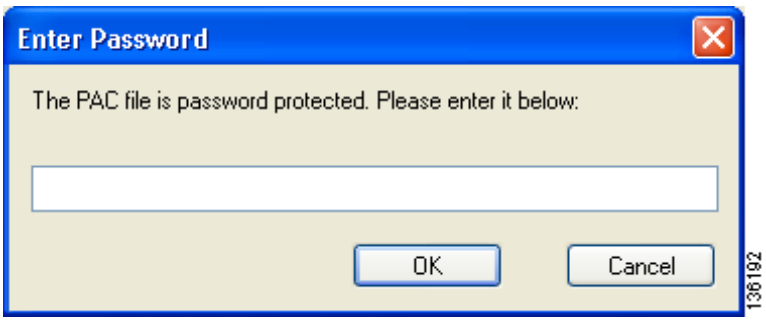
e. Click the PAC file (*.pac) so that it appears in the File name box at the bottom of the window.

Note The filename and extension of a PAC file is determined by the PAC authority that issues it, but the standard file extension is *pac*.

f. Click **Open**.

g. If the Enter Password window appears (see Figure 5-11), enter the PAC file password, which can be obtained from your system administrator, and click **OK**.

Figure 5-11 Enter Password Window



Note PAC file passwords are optional. The PAC authority determines whether to issue PAC files that require user-supplied passwords. Nevertheless, all PAC files (even those without passwords) are encrypted and protected. PAC file passwords are different from EAP-FAST passwords and need to be entered only once, at the time a PAC is imported.

h. If you try to import a PAC file with the same PAC ID as a previously imported PAC file, you are asked if you want to update the existing PAC. If you click **Yes**, the existing PAC is replaced by the new one from the imported file.

i. If the PAC file was imported successfully, the following message appears: "EAP-FAST PAC file was imported and ready for use." Click **OK** to return to the Select EAP-FAST PAC window.

j. The imported PAC now appears in the Select the PAC list on the Select EAP-FAST PAC window. Click **OK** to return to the EAP-FAST Settings window.

k. The name of the PAC authority that issued the PAC now appears in the PAC authority drop-down box on the EAP-FAST Settings window. Select the desired PAC authority from the list.

Step 11 Click **OK** to save your settings and return to the Profile Management (Security) window.

Note If you selected a private PAC and the No Network Connection Unless User Is Logged In check box is unchecked, a message appears indicating that the PAC may not be accessible during the domain logon process or when you are logged off. If you want a copy of the PAC to be added to the global store so that it will be available when you are not logged on, click **Yes**. If you do not want a copy of the PAC to be added to the global store, click **No**; then click **OK** when a message appears indicating that you may need to later reconfigure your profile to use a global PAC if you experience wireless connection problems during domain logon or when you are not logged on.

Step 12 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 13 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 14 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 15 Refer to Chapter 6 for instructions on authenticating using EAP-FAST.

Deleting a Manually Provisioned PAC File

Follow these steps if you ever want to remove a manually provisioned PAC file from storage.

Step 1 On the Select EAP-FAST PAC window, highlight the PAC file in the Select the PAC list that you want to remove from storage.

Step 2 Click **Delete**.

Step 3 When a message appears asking you to confirm your decision, click **Yes**. The PAC file is removed from the Select the PAC list.

Enabling EAP-TLS or PEAP

Before you can enable EAP-TLS or PEAP authentication, your network devices must meet the following requirements:

- You must have a valid Windows username and password, and the password cannot be blank.
- The appropriate certificates must be installed on your computer. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate.

  Note Contact your system administrator if you need help obtaining and importing the necessary certificates.

- To support EAP-TLS machine authentication with machine credentials:
  - A machine certificate must be obtained from the server, and client machine access must be enabled on the server.
  - Permissions for the MachineKeys folder, which stores the certificate pair keys for both the computer and users, must be set correctly. Refer to Microsoft knowledgebase article Q278381 for information on correctly setting up folder permissions:

    http://support.microsoft.com/default.aspx?scid=kb;en-us;Q278381

    Note If you ever change permissions on higher-level directories and those settings are applied to all subdirectories, you may need to reset the permissions for the MachineKeys folder.

- To use WPA2 with EAP-TLS or PEAP authentication, client adapters must use the software included in Install Wizard 2.0 or later.
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 12.00T (access points running VxWorks), Cisco IOS Release 12.2(4)JA (1100 series access points), Cisco IOS Release 12.2(8)JA (1200 series access points), or Cisco IOS Release 12.2(13)JA (350 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later.

- All necessary infrastructure devices (such as access points, servers, gateways, user databases, etc.) must be properly configured for the authentication type you plan to enable on the client.

Follow the instructions in one of the sections below to enable EAP-TLS or PEAP authentication for this profile:

- Enabling EAP-TLS, 5-40
- Enabling PEAP (EAP-GTC), 5-42
- Enabling PEAP (EAP-MSCHAP V2), 5-46
- Enabling PEAP (EAP-MSCHAP V2) machine authentication with machine certificates, 5-49

Enabling EAP-TLS

Follow the steps below to enable EAP-TLS authentication for this profile.

Step 1 Perform one of the following on the Profile Management (Security) window:

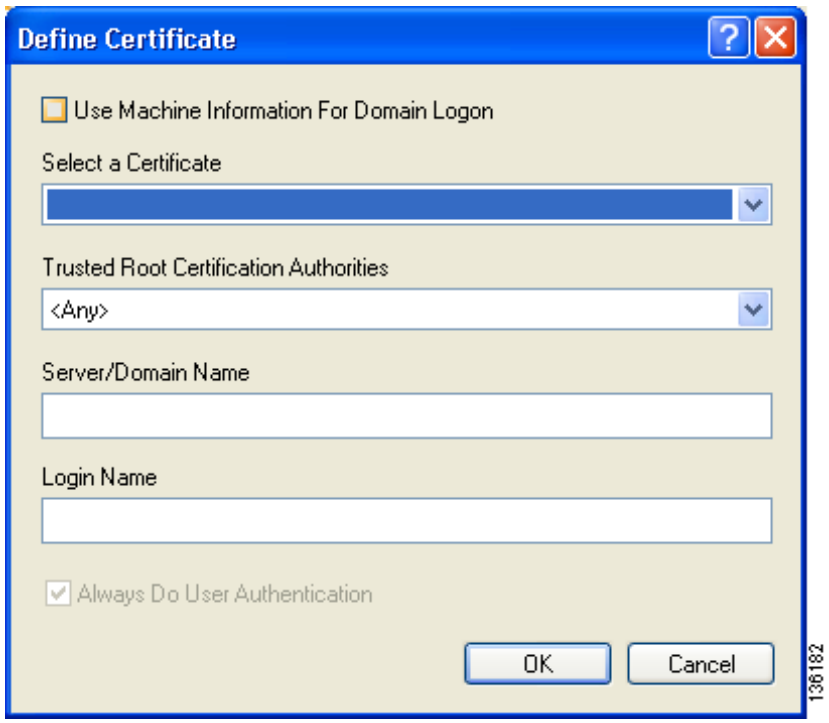
- If you want to enable EAP-TLS without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-TLS** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-TLS with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-TLS** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-18 for additional information.

Step 2 Click **Configure**. The Define Certificate window appears (see Figure 5-12).

Figure 5-12 Define Certificate Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 4 If you checked the Use Machine Information For Domain Logon check box in the previous step, the Always Do User Authentication check box at the bottom of the window becomes active. Perform one of the following:

- Check the **Always Do User Authentication** check box if you want the client to switch from using machine authentication to using user authentication after you log on using your username and password. This is the default setting.
- Uncheck the **Always Do User Authentication** check box if you want the client to continue to use machine authentication after your computer logs into the domain.

Step 5 Choose your server certificate in the Select a Certificate drop-down box.

Step 6 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.

Step 7 Perform one of the following:

- Leave the Server/Domain Name field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box. This is the recommended option.
- In the Server/Domain Name field, enter the domain name of the server from which the client will accept a certificate.

Step 8 If the Login Name field is not filled in automatically, enter your username in this format: *username@domain* (for example, jsmith@acs-test.cisco.com).

Step 9 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 10 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 11 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 13 Refer to Chapter 6 for instructions on authenticating using EAP-TLS.

Enabling PEAP (EAP-GTC)

Follow the steps below to enable PEAP (EAP-GTC) for this profile.

Step 1 Perform one of the following:

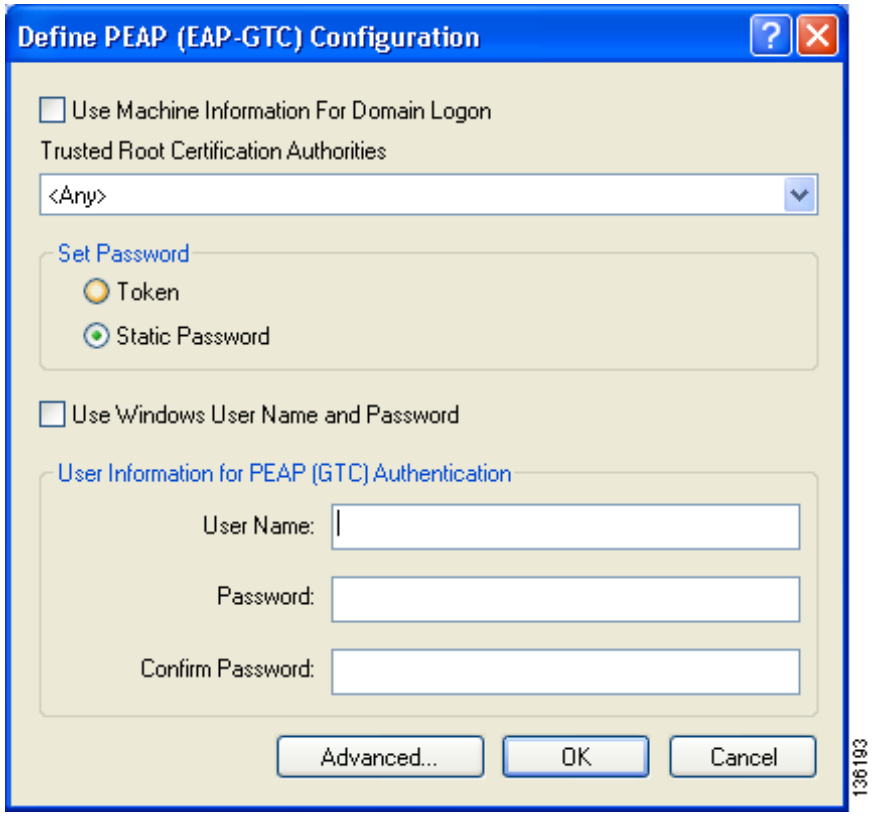
- If you want to enable PEAP (EAP-GTC) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-GTC)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-GTC) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-GTC)** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-18 for additional information.

Step 2 Click **Configure**. The Define PEAP (EAP-GTC) Configuration window appears (see Figure 5-13).

Figure 5-13 Define PEAP (EAP-GTC) Configuration Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is checked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 4 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.

Step 5 Choose either **Token** or **Static Password**, depending on your user database.

Note If you choose Token, you must use a hardware token device or the Secure Computing SofToken program (release 2.1 or later) to obtain the one-time password and enter the password when prompted during the authentication process. Secure Computing PremierAccess release 3.1.1 or later is the only supported token server.

Step 6 Perform one of the following to specify the username that will be used for inner PEAP tunnel authentication:

- If you want your Windows username to also serve as your PEAP username, check the **Use Windows User Name** check box. This option gives you only one username to remember.

Note If you chose the Static Password option in Step 5, the check box reads *Use Windows User Name and Password*.

- If you want to enter a separate PEAP username (which is registered with the RADIUS server) in addition to your regular Windows username in order to start the PEAP authentication process, enter your PEAP username in the User Name field.

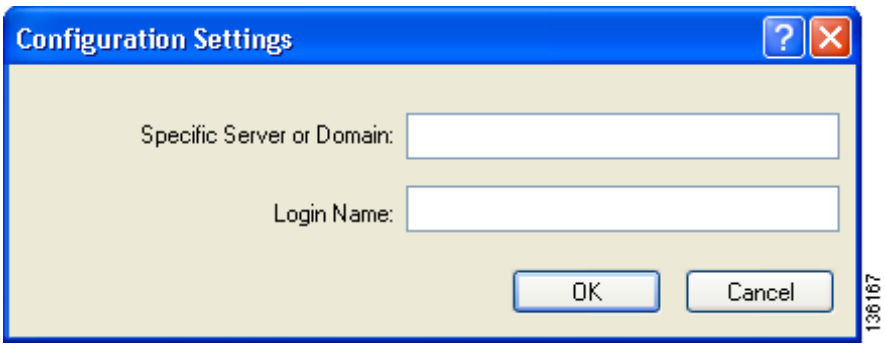
Note Your Windows username is filled in automatically. Simply delete your Windows username and enter your separate PEAP username.

Step 7 If you entered a PEAP username in the previous step and chose the Static Password option in Step 5, enter your PEAP authentication password (which is registered with the RADIUS server) in both the Password and Confirm Password fields.

Step 8 If the Use Windows User Name and Password check box is unchecked and you want to implement added security by further refining the network certificate that will be accepted and controlling the string used to set up the outer PEAP tunnel, follow these steps:

a. Click **Advanced**. The Configuration Settings window appears (see Figure 5-14).

Figure 5-14 Configuration Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box on the Define PEAP (EAP-GTC) Configuration window (this is the recommended option) or enter the domain name of the server from which the client will accept a certificate.

c. If the Login Name field is not filled in automatically, enter your username with nothing after it (for example, jsmith).

d. Click **OK** to save your settings.

Step 9 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 10 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 11 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 13 Refer to Chapter 6 for instructions on authenticating using PEAP (EAP-GTC).

Enabling PEAP (EAP-MSCHAP V2)

Follow the steps below to enable PEAP (EAP-MSCHAP V2) for this profile.

Step 1 Perform one of the following:

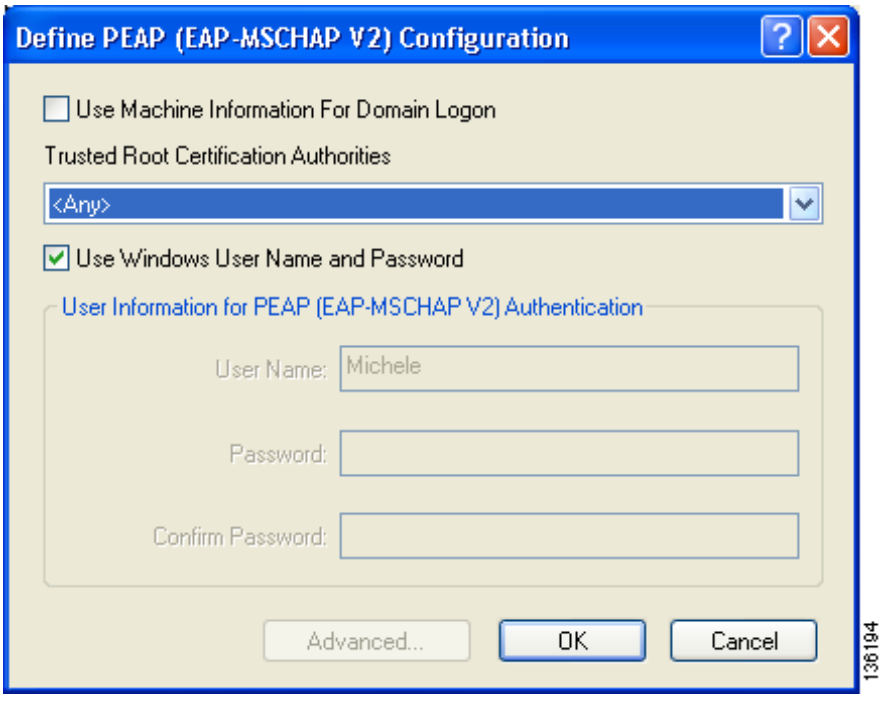
- If you want to enable PEAP (EAP-MSCHAP V2) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-MSCHAP V2) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-18 for additional information.

Step 2 Click **Configure**. The Define PEAP (EAP-MSCHAP V2) Configuration window appears (see Figure 5-15).

Figure 5-15 Define PEAP (EAP-MSCHAP V2) Configuration Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is checked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 4 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.

Step 5 Perform one of the following to specify the username and password that will be used for inner PEAP tunnel authentication:

- If you want your Windows username and password to also serve as your PEAP username and password, check the **Use Windows User Name and Password** check box.
- If you want to use a distinct username and password (which are registered with the RADIUS server) to start the PEAP authentication process, follow these steps:

  a. Enter your PEAP username and password in the corresponding fields.

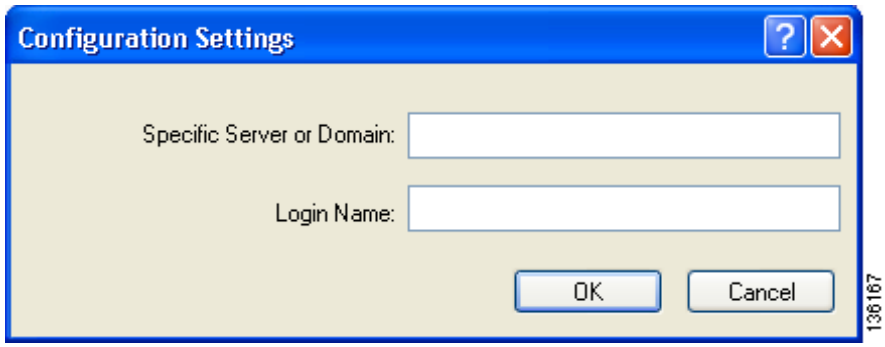
  Note Your Windows username is filled in automatically. Simply delete your Windows username and enter your separate PEAP username.

  b. Re-enter your password in the Confirm Password field.

Step 6 If the Use Windows User Name and Password check box is unchecked and you want to implement added security by further refining the network certificate that will be accepted and controlling the string used to set up the outer PEAP tunnel, follow these steps:

a. Click **Advanced**. The Configuration Settings window appears (see Figure 5-16).

Figure 5-16 Configuration Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box on the Define PEAP (EAP-MSCHAP V2) Configuration window (this is the recommended option) or enter the domain name of the server from which the client will accept a certificate.

c. If the Login Name field is not filled in automatically, enter your username with nothing after it (for example, jsmith).

Note Some RADIUS servers require that the same name be entered for both the inner and outer PEAP tunnels. That is, the same name may need to be entered in both the Login Name field and the User Name field on the Define PEAP (EAP-MSCHAP V2) Configuration window. Contact your system administrator for information.

d. Click **OK** to save your settings.

Step 7 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 8 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 9 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 10 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 11 Refer to Chapter 6 for instructions on authenticating using PEAP (EAP-MSCHAP V2).

Enabling PEAP (EAP-MSCHAP V2) Machine Authentication with Machine Credentials

The Host Based EAP option in the 802.1x EAP Type drop-down box on the Profile Management (Security) window enables client adapters that are configured through ADU to attempt to log into a domain using PEAP (EAP-MSCHAP V2) machine authentication with machine credentials. Doing so enables your computer to connect to the network prior to user logon. Follow these steps to enable this authentication type.

Note This procedure enables you to use PEAP (EAP-MSCHAP V2) machine authentication with *machine* credentials. If you want to enable PEAP (EAP-MSCHAP V2) machine authentication with *user* credentials, follow the instructions in the "Enabling PEAP (EAP-MSCHAP V2)" section on page 5-46.

Note Because this feature requires the Microsoft Wireless Configuration Manager to start and stop as you switch between host-based EAP and non-host-based EAP profiles, it works only for users with administrator or power-user privileges. An error message appears if you attempt to switch to or from a host-based EAP profile and you do not have the proper permissions.

Note To use this feature on a computer running Windows 2000, your computer must have the Microsoft 802.1X supplicant installed.

Note Host Based EAP is not included in the list of WPA/WPA2/CCKM EAP Type options on the Profile Management (Security) window in ADU because this feature is not supported for use with WPA or WPA2.

Step 1 Choose **802.1x** under Set Security Options and **Host Based EAP** in the 802.1x EAP Type drop-down box.

Step 2 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section on page 3-20 for information on obtaining and installing the hot fix.

Step 3 Click **OK** to save your settings.

Step 4 Activate this profile on the Cisco Aironet Desktop Utility (Profile Management) window. The Microsoft Wireless Configuration Manager starts.

Step 5 Click **Start** > **Settings** > **Control Panel** > **Network and Dial-up Connections** or **Network Connections**.

Step 6 Right-click your wireless connection.

Step 7 Click **Properties**. The Connection Properties window appears.

Step 8 Perform one of the following:

- On Windows 2000, click the **Authentication** tab.
- On Windows XP, choose the **Wireless Networks** tab, make sure that the **Use Windows to configure my wireless network settings** check box is checked, click the SSID of the access point to which you want the client adapter to associate from the list of available networks, click **Configure**, and choose the **Authentication** tab.

Step 9 For EAP type, choose **Protected EAP (PEAP)**.

Step 10 Configure any applicable settings on the Protected EAP Properties window and subwindows.

Note Refer to the "Enabling PEAP (EAP-MSCHAP V2)" section on page E-14 if you need help configuring the PEAP (EAP-MSCHAP V2) settings.

Step 11 After you have finished the configuration, PEAP authentication should begin. Depending on the configuration settings you selected, you may be prompted for your PEAP username, password, and domain name. Note that you may need to minimize ADU in order to access the pop-up window that prompts you for your credentials.

Note You can have multiple host-based EAP profiles in ADU, but the Microsoft Wireless Configuration Manager maintains only one configuration. If you want to use different PEAP property settings for different host-based EAP profiles, you need to repeat the previous steps beginning with Step 4 every time you switch to a different host-based EAP profile.

Note When you activate a host-based EAP profile, the Microsoft Wireless Configuration Manager takes control of the client adapter's authentication attempt. However, when you activate a non-host-based EAP profile, ADU assumes this control.

Note If you experience problems while using a host-based EAP profile, make sure that 802.1X authentication is disabled for any other network connection.

Disabling Static WEP, WPA/WPA2 Passphrase, or EAP

To disable static WEP, WPA/WPA2 passphrase, or EAP authentication [LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2)] for a particular profile, choose **None** on the Profile Management (Security) window and click **OK**.

Note Choosing any security option other than Pre-Shared Key (Static WEP) on the Profile Management (Security) window disables static WEP automatically.

Note Choosing **Pre-Shared Key (Static WEP)** or **WPA/WPA2 Passphrase** on the Profile Management (Security) window disables EAP automatically.

Enabling Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). It specifically supports priority tagging and queuing. QoS is an access point feature that enables networking professionals to provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. Implementing QoS in a wireless LAN makes network performance more predictable and bandwidth usage more effective.

Cisco recommends that you enable WMM if your computer is running a time-sensitive application for QoS-aware clients such as voice or video (for example, Cisco IP SoftPhone).

QoS and WMM must be enabled on the access point to which the client will associate. These features are supported on the access point in Cisco IOS Release 12.3(2)JA or later. Refer to the documentation for your access point for instructions on enabling these features.

WMM is supported automatically on the client adapter in the software included in Install Wizard 2.0 or later. However, you must enable the Windows QoS Packet Scheduler to ensure WMM support. Follow the instructions below to enable the QoS Packet Scheduler on Windows 2000 or XP.

Note The QoS Packet Scheduler must be installed before you can enable it. It comes preinstalled on Windows XP; however, you must install it on Windows 2000.

Enabling the QoS Packet Scheduler on Windows 2000

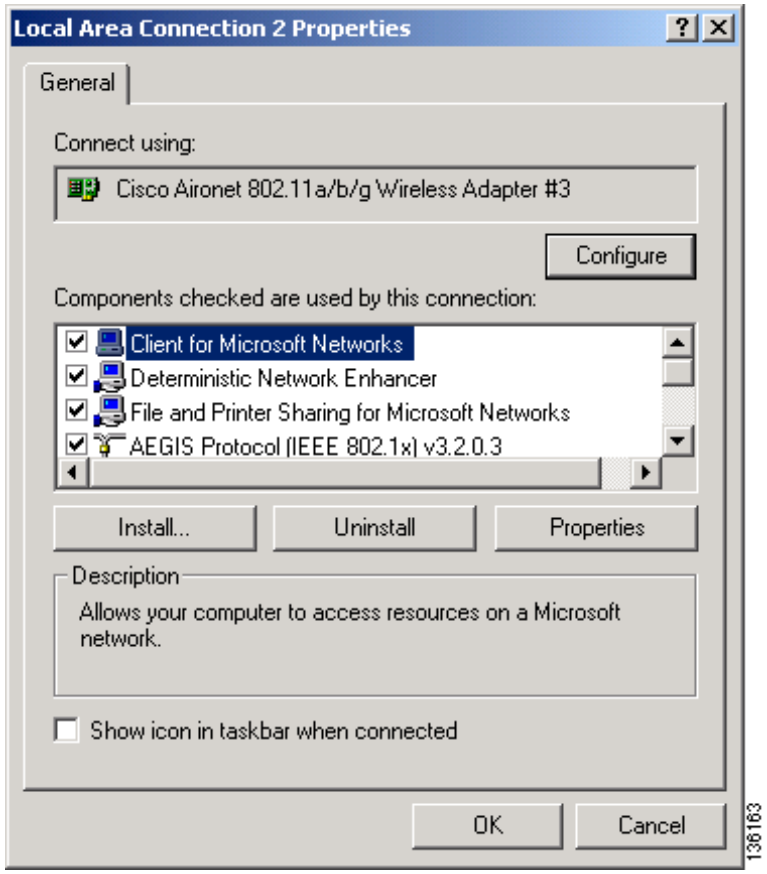
Follow these steps to enable the QoS Packet Scheduler on a computer running Windows 2000.

Step 1 Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.

Step 2 Right-click your wireless network connection.

Step 3 Click **Properties**. The Wireless Cisco Connection Properties window appears (see Figure 5-17).

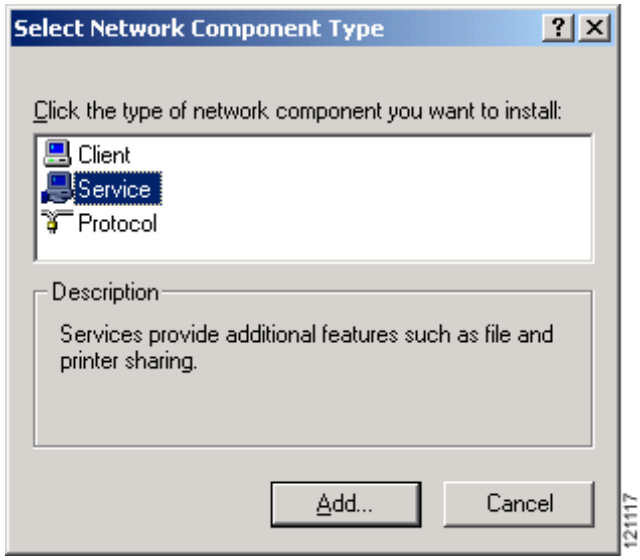
Figure 5-17 Wireless Cisco Connection Properties Window



Step 4 If the QoS Packet Scheduler is already installed, it is included in the list of components that this connection uses. If it appears in the list, go to Step 8. Otherwise, go to the next step to install it.

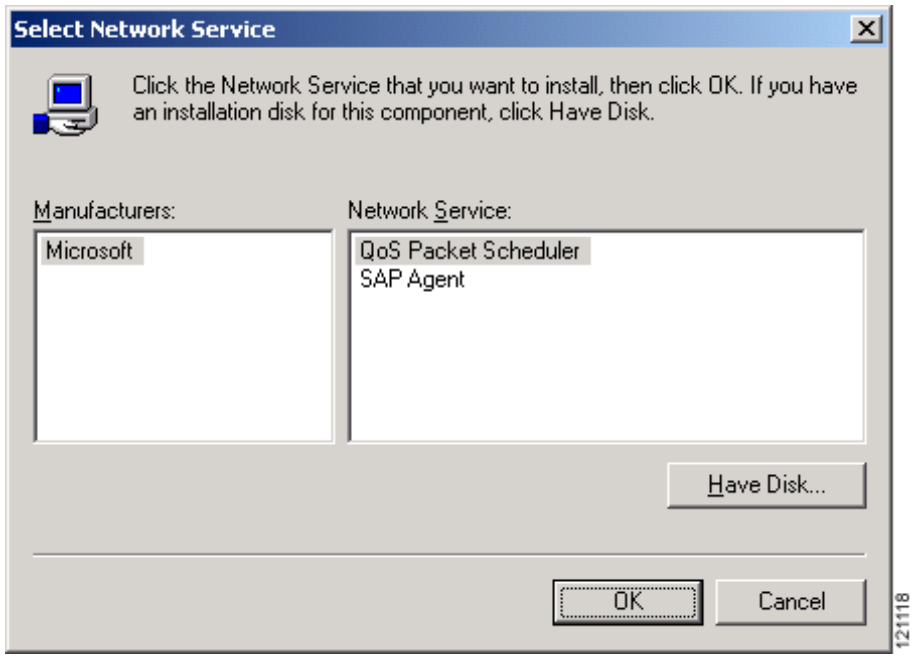
Step 5 Click **Install**. The Select Network Component Type window appears (see Figure 5-18).

Figure 5-18 Select Network Component Type Window



Step 6 Choose **Service** and click **Add**. The Select Network Service window appears (see Figure 5-19).

Figure 5-19 Select Network Service Window



Step 7 Click **QoS Packet Scheduler** and **OK**. The Wireless Cisco Connection Properties window reappears, and the QoS Packet Scheduler is included in the list of connections.

Step 8 Check the **QoS Packet Scheduler** check box if it is not checked.

Step 9 Click **OK**.

Enabling the QoS Packet Scheduler on Windows XP

Follow these steps to enable the QoS Packet Scheduler on a computer running Windows XP.

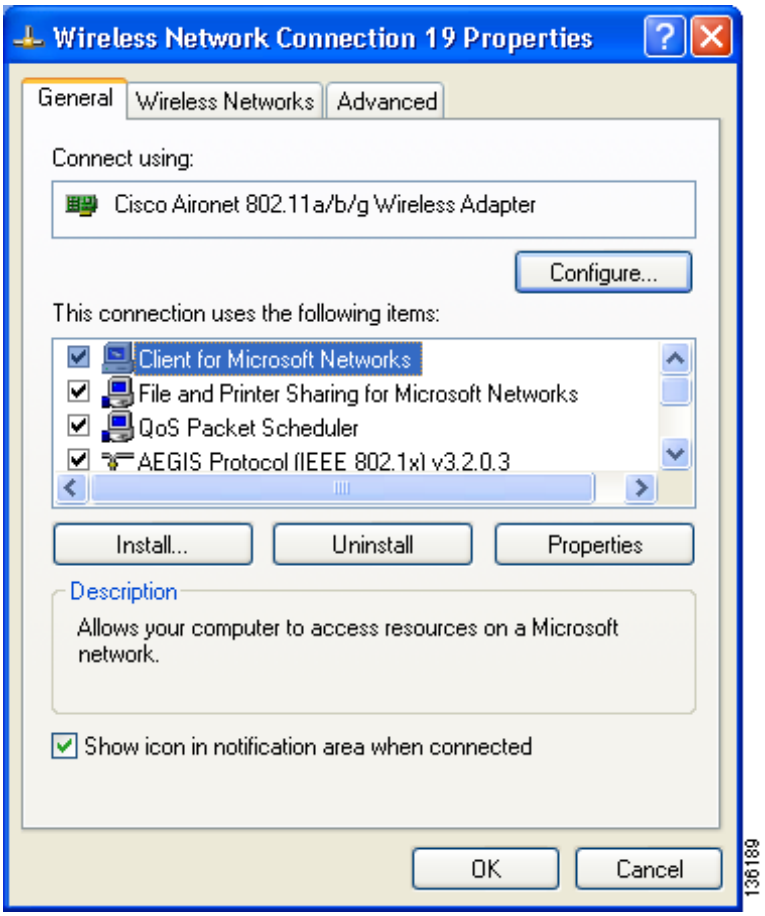
Step 1 Click **Control Panel**.

Step 2 Double-click **Network Connections**.

Step 3 Right-click your wireless network connection.

Step 4 Click **Properties**. The Wireless Network Connection Properties window appears (see Figure 5-20).

Figure 5-20 Wireless Network Connection Properties Window



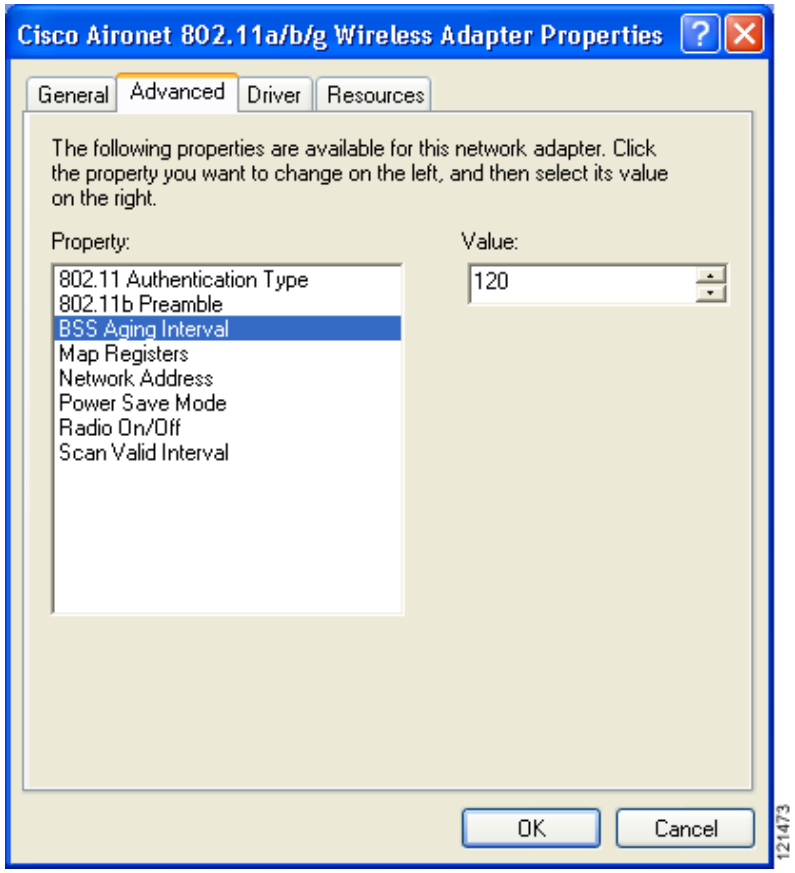
Step 5 Check the **QoS Packet Scheduler** check box, which appears in the list of items that this connection uses.

Step 6 Click **OK**.

Setting Roaming Parameters in the Windows Control Panel

The Cisco Aironet 802.11a/b/g Wireless Adapter Properties window (see Figure 5-21) in the Windows Control Panel enables you to set two parameters that regulate the client adapter's roaming capabilities.

Figure 5-21 Cisco Aironet 802.11a/b/g Wireless Adapter Properties Window



Follow these steps to access the roaming parameters.

Step 1 Double-click **My Computer**, **Control Panel**, and **System**.

Step 2 Click the **Hardware** tab and **Device Manager**.

Step 3 Double-click **Network Adapters**.

Step 4 Right-click **Cisco Aironet 802.11a/b/g Wireless Adapter**.

Step 5 Click **Properties** and the **Advanced** tab. The roaming parameters appear in the Property list. Table 5-5 lists and describes the client adapter's roaming parameters. Follow the instructions in the table to change the parameters.

Table 5-5 Roaming Parameters (in the Windows Control Panel)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>BSS Aging Interval</td><td>The amount of time (in seconds) that the client keeps an access point in its roaming scanlist after it can no longer communicate to that device. The higher the value, the greater the number of access points to which the client may roam.

Range: 20 to 300 seconds (in 10-second increments)

Default: 120 seconds

Note Cisco recommends that you set the BSS Aging Interval to twice the value of the Scan Valid Interval. For example, if the Scan Valid Interval is 50, the BSS Aging Interval would be 100.</td></tr>
<tr><td>Scan Valid Interval</td><td>The amount of time (in seconds) before the client starts scanning for a better access point after reaching the roaming threshold or missing beacons. (See the threshold criteria in the table below.) The higher the value, the less time the client spends scanning for a better access point and the more time it has to send data.

Range: 20 to 120 seconds (in 5-second increments)

Default: 60 seconds

Note The client does not scan for a new access point as long as it has a good connection and is passing data.

<table>
<tr><th>Wireless Mode</th><th>Signal Strength Threshold (dBm)</th><th>Transmit Rate Threshold (Mbps)</th></tr>
<tr><td>5 GHz, 54 Mbps or
2.4 GHz, 54 Mbps</td><td>24</td><td>24</td></tr>
<tr><td>2.4 GHz, 11 Mbps
(other modes enabled)</td><td>24</td><td>9</td></tr>
<tr><td>2.4 GHz, 11 Mbps
(only mode enabled)</td><td>24</td><td>5</td></tr>
</table>
</td></tr>
</table>

Using EAP Authentication

This chapter explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is activated.

The following topics are covered in this chapter:

- Overview, page 6-2
- Using LEAP or EAP-FAST, page 6-2
- Using LEAP or EAP-FAST with the Windows Username and Password, page 6-3
- Using LEAP or EAP-FAST with an Automatically Prompted Login, page 6-5
- Using LEAP or EAP-FAST with a Manually Prompted Login, page 6-8
- Using LEAP or EAP-FAST with a Saved Username and Password, page 6-12
- Using EAP-TLS, page 6-13
- Using PEAP (EAP-GTC), page 6-14
- Using PEAP (EAP-MSCHAP V2), page 6-15
- Restarting the Authentication Process, page 6-15

Overview

This chapter explains the sequence of events that occurs after you (or auto profile selection) activate a profile that uses EAP authentication or you eject and reinsert the client adapter, reboot the computer, log on while this profile is active, or are informed that your password has expired or is invalid. The chapter contains seven sections based on the profile's authentication type and its username and password settings:

- LEAP or EAP-FAST with the Windows username and password, page 6-3
- LEAP or EAP-FAST with an automatically prompted login, page 6-5
- LEAP or EAP-FAST with a manually prompted login, page 6-8
- LEAP or EAP-FAST with a saved username and password, page 6-12
- EAP-TLS, page 6-13
- PEAP (EAP-GTC), page 6-14
- PEAP (EAP-MSCHAP V2), page 6-15

Also provided are an overview of LEAP and EAP-FAST authentication (below) and instructions for restarting the authentication process when necessary (page 6-15).

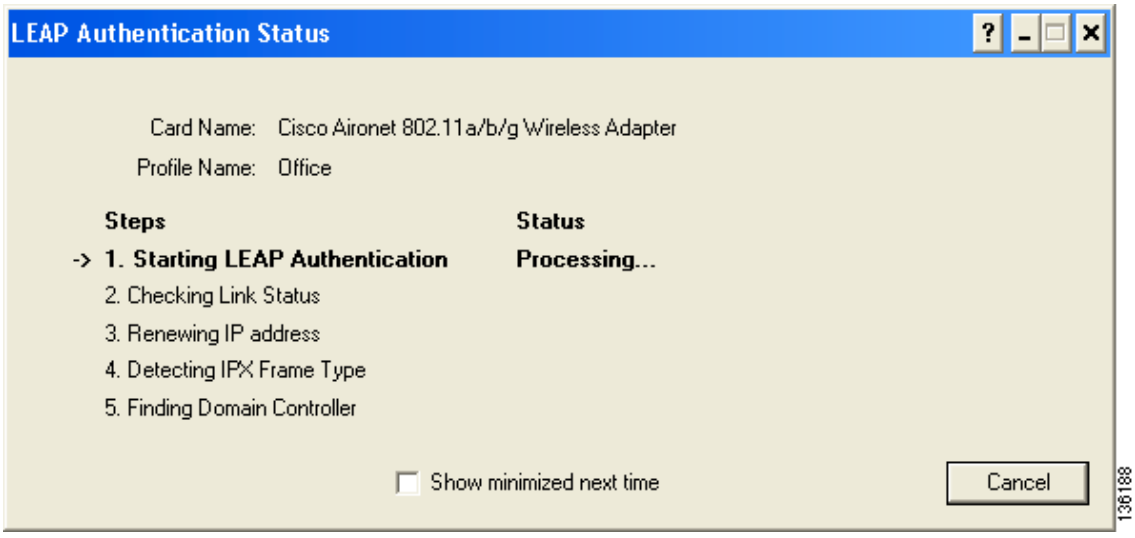
Follow the instructions for your profile's authentication type and credential settings to successfully authenticate.

Note If any error messages appear during authentication, refer to Chapter 10 for explanations and recommended actions.

Using LEAP or EAP-FAST

When LEAP or EAP-FAST authentication begins, the LEAP or EAP-FAST Authentication Status window appears (see Figure 6-1).

Figure 6-1 LEAP or EAP-FAST Authentication Status Window



This window provides information about the status of LEAP or EAP-FAST authentication. Table 6-1 lists and explains the stages of LEAP or EAP-FAST authentication. As each stage is completed, a status message (such as *Success)* appears in the Status field. If any error messages appear, refer to the "Error Messages" section on page 10-12 for an explanation and the recommended action to take.

Table 6-1 Stages of LEAP or EAP-FAST Authentication

Stage	Explanation
Starting LEAP or EAP-FAST Authentication	The client adapter associates to an access point, and the LEAP or EAP-FAST authentication process begins.
Checking Link Status	The client adapter is EAP authenticated, and the network connection is verified.
Renewing IP Address	If DHCP is enabled, the IP address is released and renewed.
Detecting IPX Frame Type	The IPX frame type is reset if AutoDetect is enabled.
Finding Domain Controller	If you are logging into a domain and the active profile specifies that the domain name be included, an attempt is made to find the domain controller to make sure subsequent access to the domain is successful.

If you do not want the LEAP or EAP-FAST Authentication Status window to appear each time the client adapter attempts to authenticate using LEAP or EAP-FAST, check the **Show minimized next time** check box at the bottom of the window. On future LEAP or EAP-FAST authentication attempts, the LEAP or EAP-FAST Authentication Status window appears minimized in the Windows taskbar.

Note To make the LEAP or EAP-FAST Authentication Status window reappear once it has been minimized, click the **LEAP Authentication Status** or **EAP-FAST Authentication Status** tab in the Windows taskbar and uncheck the **Show minimized next time** check box. The LEAP or EAP-FAST Authentication Status window should now appear for all future LEAP or EAP-FAST authentication attempts.

Using LEAP or EAP-FAST with the Windows Username and Password

After Profile Activation or Card Insertion

After you (or auto profile selection) activate a profile that uses your Windows username and password for LEAP or EAP-FAST authentication or you eject and reinsert the client adapter while this profile is active, the following events occur:

1. The LEAP or EAP-FAST Authentication Status window appears.
2. If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

3. If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

   If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After a Reboot or Logon

After your computer reboots or you log on, follow these steps to authenticate using LEAP or EAP-FAST.

Step 1 When the Windows login window appears, enter your Windows username and password and click **OK**. The domain name is optional.

Note If your computer has Novell Client 32 software installed, a separate LEAP or EAP-FAST login window appears before the Novell login window. If this occurs, enter your Windows and Novell username and password in the login windows and click **OK**.

The LEAP or EAP-FAST Authentication Status window appears.

Step 2 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 3 If your client adapter authenticates, the window shows that each stage was successful and then disappears.

If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

Step 4 Windows continues to log you onto the system. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

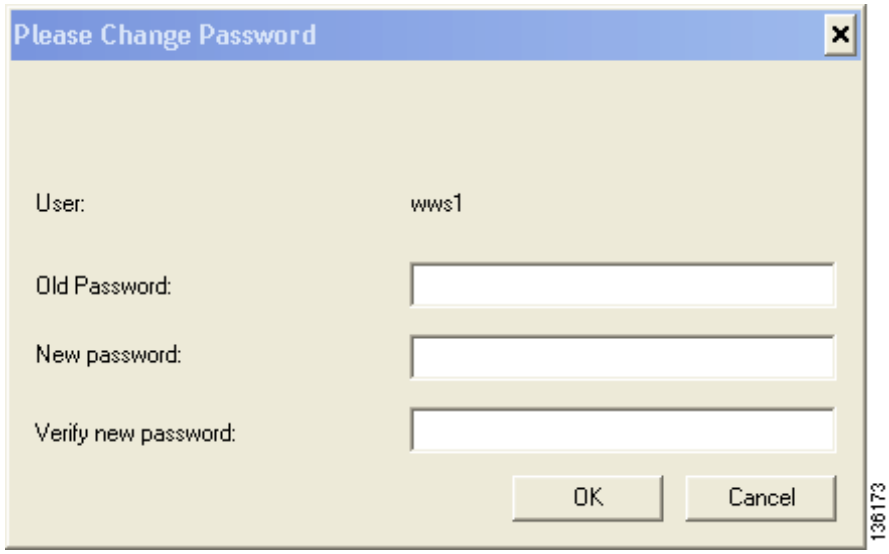
After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Note If you change your Windows password using the standard Windows Change Password function, the client updates the EAP-FAST password automatically and maintains its connection to the access point if the current profile uses the Windows username and password. However, data packets may be dropped during this process.

Step 1 When the Please Change Password window appears (see Figure 6-2) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-2 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields and click **OK**.

Step 3 If prompted, log off and on again in order to update your local cached account with your new password.

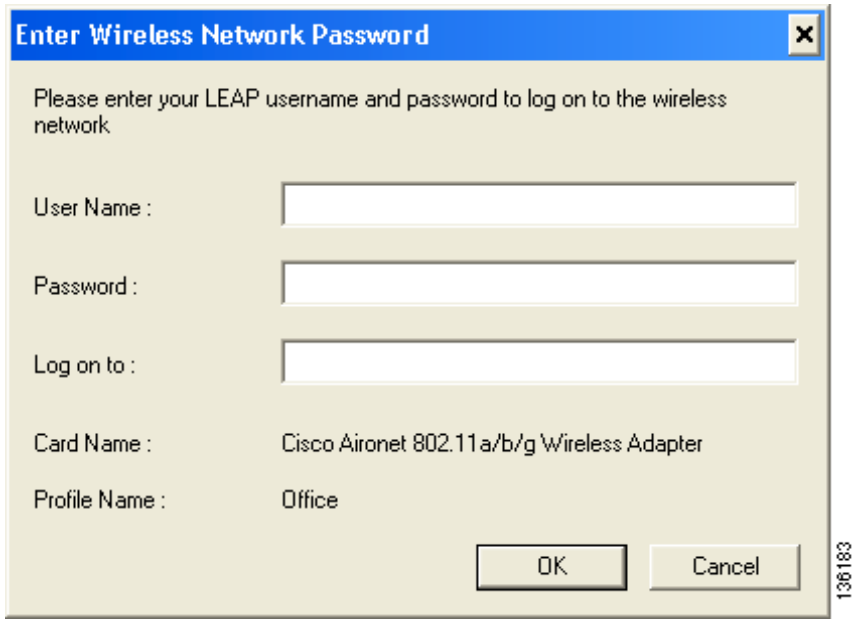
Using LEAP or EAP-FAST with an Automatically Prompted Login

After Profile Activation or Card Insertion

After you (or auto profile selection) activate a profile that uses a separate username and password for LEAP or EAP-FAST authentication or you eject and reinsert the client adapter while this profile is active, follow these steps to authenticate.

Step 1 When the Enter Wireless Network Password window appears (see Figure 6-3), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-3 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 2 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 3 If your client adapter authenticates, the LEAP or EAP -FAST Authentication Status window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

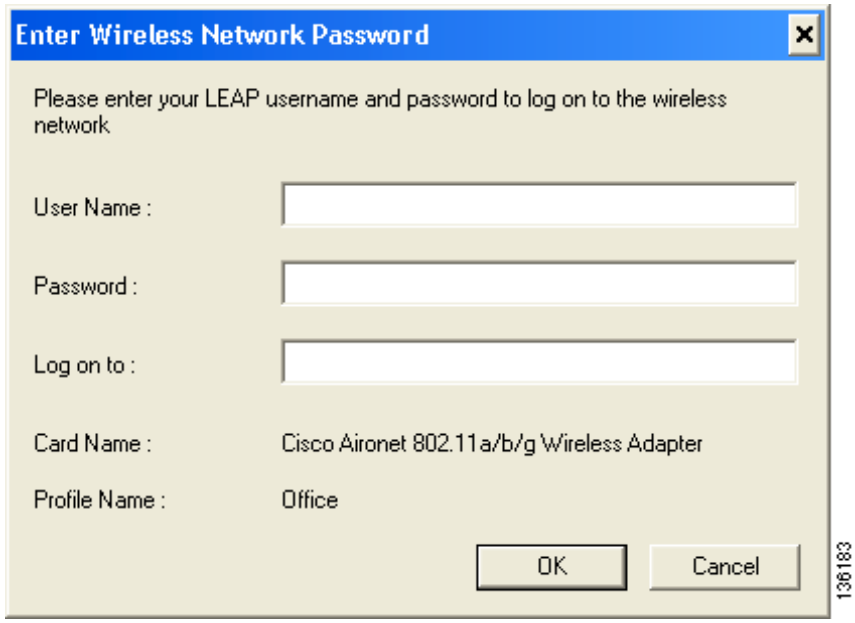
After a Reboot or Logon

After your computer reboots or you log on, follow these steps to authenticate using LEAP or EAP-FAST.

Step 1 When the Windows login window appears, enter your Windows username and password and click **OK**.

Step 2 When the Enter Wireless Network Password window appears (see Figure 6-4), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-4 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 3 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 4 If your client adapter authenticates, the window shows that each stage was successful and then disappears. The logon or boot-up process completes.

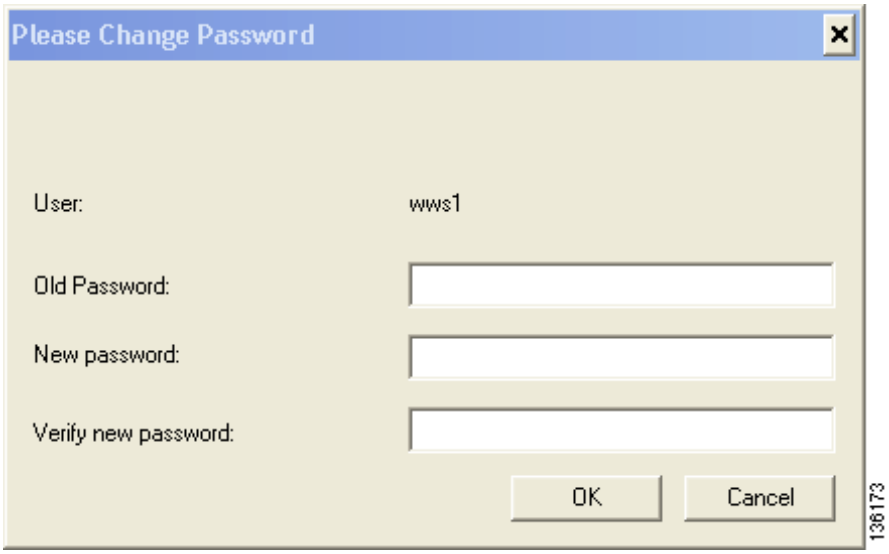
If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Step 1 When the Please Change Password window appears (see Figure 6-5) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-5 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields.

Step 3 Click **OK**. The client adapter should authenticate using your new password.

Using LEAP or EAP-FAST with a Manually Prompted Login

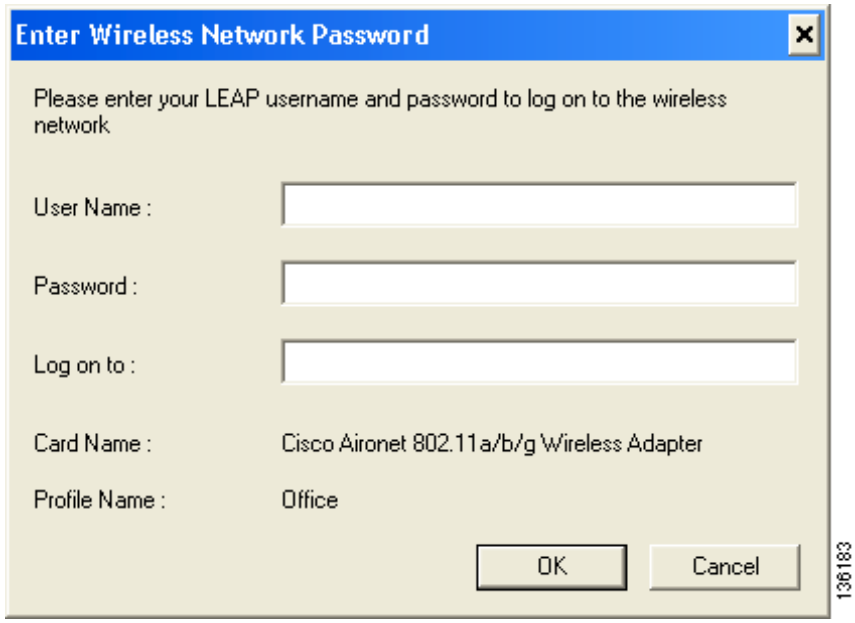
After Profile Activation

After you (or auto profile selection) activate a profile that uses LEAP or EAP-FAST authentication with a manually prompted login, follow these steps to authenticate.

Note If auto profile selection is enabled, this procedure is applicable the first time auto profile selection activates a manual LEAP or manual EAP-FAST profile. After you follow these steps to enter your LEAP or EAP-FAST credentials, you can switch profiles without having to re-enter your credentials until you reboot your computer, eject and reinsert your client adapter, or change the profile in any way (including its priority in auto profile selection). If auto profile selection is disabled, you must re-enter your credentials every time you activate a manual LEAP or manual EAP-FAST profile.

Step 1 When the Enter Wireless Network Password window appears (see Figure 6-6), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-6 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 2 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 3 If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

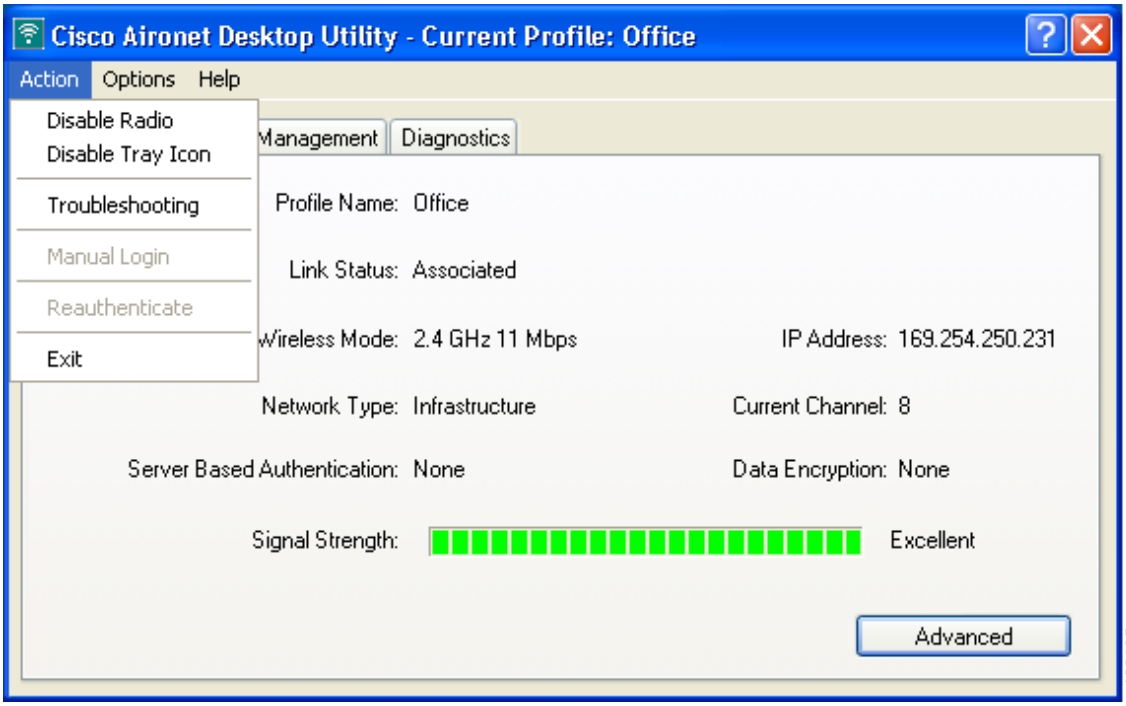
After a Reboot, Logon, or Card Insertion

After your computer reboots, you log on, or you eject and reinsert the client adapter, the adapter does not automatically attempt to authenticate. You must manually invoke the authentication process. To do so, follow these steps.

Step 1 If you rebooted your computer or logged on, complete your standard Windows login. Then open ASTU or ADU.

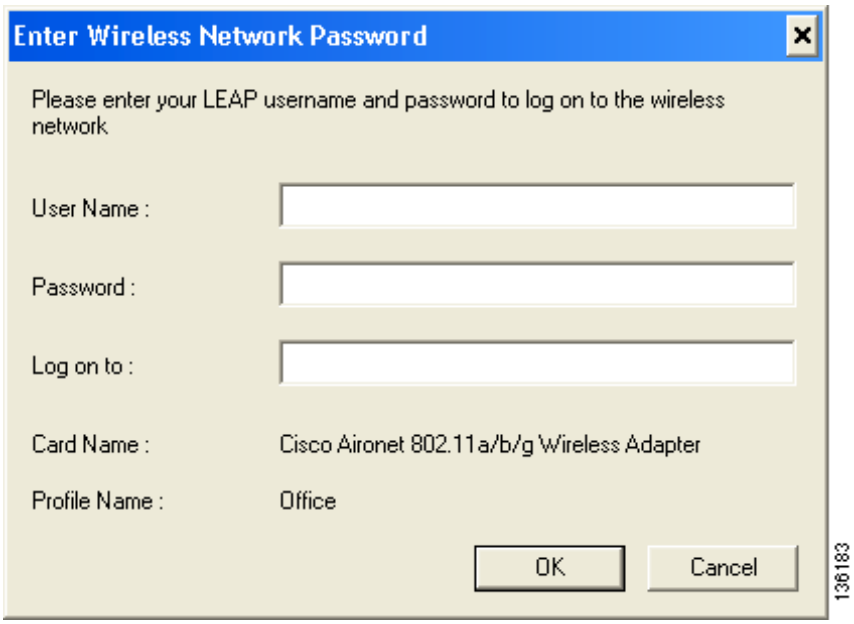
Step 2 Choose the **Manual Login** option from the ASTU pop-up menu or the ADU Action drop-down menu (see Figure 6-7).

Figure 6-7 Action Drop-Down Menu



Step 3 When the Enter Wireless Network Password window appears (see Figure 6-8), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-8 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 4 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 5 If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

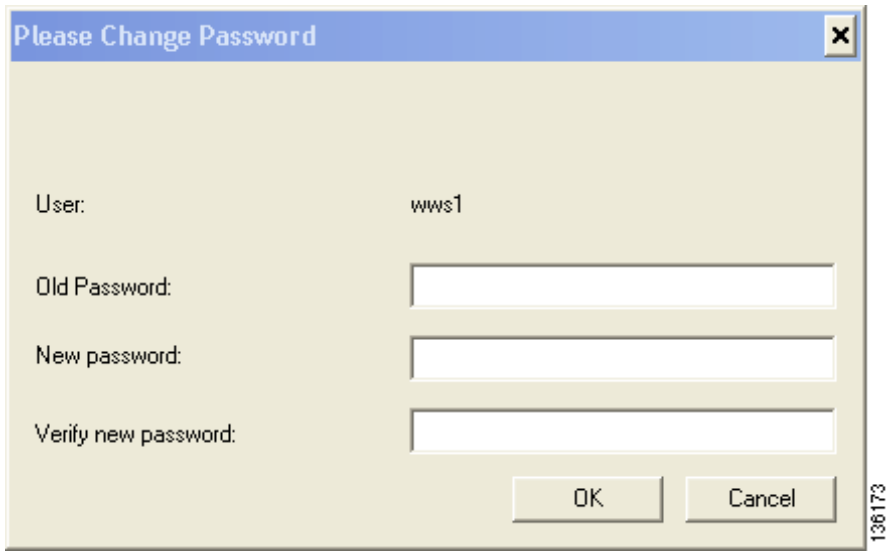
If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Step 1 When the Please Change Password window appears (see Figure 6-9) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-9 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields.

Step 3 Click **OK**. The client adapter should authenticate using your new password.

Using LEAP or EAP-FAST with a Saved Username and Password

After Profile Activation or Card Insertion

After you (or auto profile selection) activate a profile that uses LEAP or EAP-FAST authentication with a saved LEAP or EAP-FAST username and password or you eject and reinsert the client adapter while this profile is active, the following events occur:

1. The LEAP or EAP-FAST Authentication Status window appears.
2. If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.
3. If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

   If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After a Reboot or Logon

After your computer reboots or you log on, the following events occur:

1. After you enter your Windows username and password, the authentication process begins automatically using your saved LEAP or EAP-FAST username and password.

   Note If you unchecked the **No Network Connection Unless User Is Logged In** check box on the LEAP Settings window or EAP-FAST Settings window, the EAP authentication process begins before the Windows login window appears.

2. If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.
3. If your client adapter authenticates, the LEAP or EAP-FAST Authentication Status window shows that each stage was successful and then disappears.

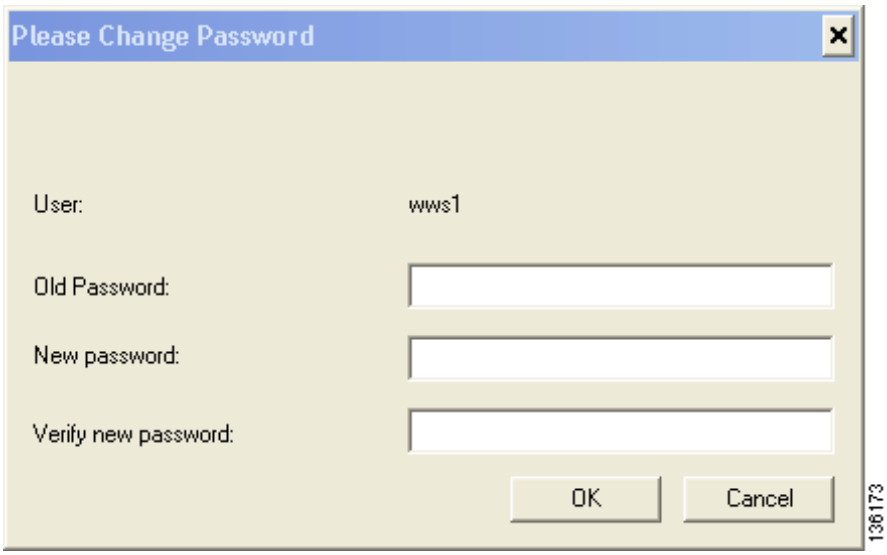
   If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.
4. Windows continues to log you onto the system. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Step 1 When the Please Change Password window appears (see Figure 6-10) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-10 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields.

Step 3 Click **OK**. The client adapter should authenticate using your new password.

Step 4 Edit the profile in ADU by changing the saved username and password on the EAP-FAST Settings window.

Using EAP-TLS

After you (or auto profile selection) activate a profile that uses EAP-TLS authentication or you eject and reinsert the client adapter, reboot the computer, or log on while this profile is active, the EAP authentication process begins automatically, and the client adapter should EAP authenticate.

If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

Using PEAP (EAP-GTC)

After you (or auto profile selection) activate a profile that uses PEAP (EAP-GTC) authentication or you eject and reinsert the client adapter, reboot the computer, or log on while this profile is active, follow the steps in one of the sections below to EAP authenticate. Choose the section appropriate for your user database.

Windows NT or 2000 Domain Databases or LDAP Databases Only

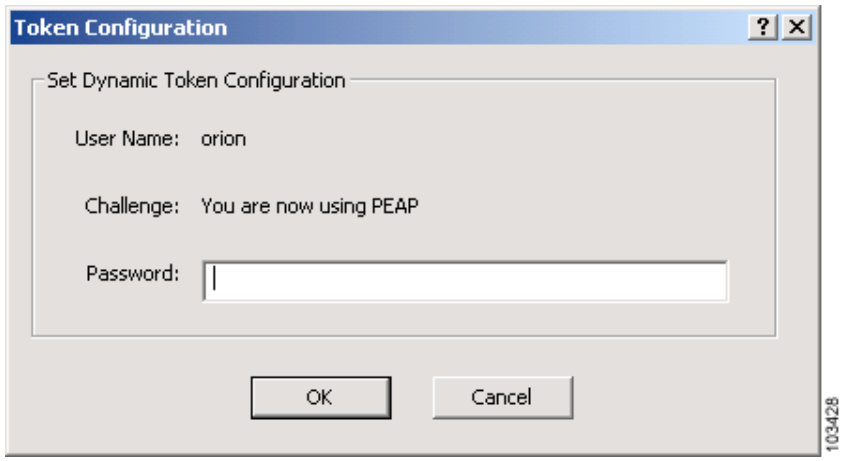
The EAP authentication process begins automatically. The client adapter should EAP authenticate using either your Windows credentials or the username and password entered in the Define PEAP (EAP-GTC) Configuration window. If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

OTP Databases Only

Step 1 Use your hardware token device or SofToken program to obtain the one-time password.

Step 2 When the Token Configuration window appears (see Figure 6-11), enter the one-time password.

Figure 6-11 Token Configuration Window



Note The username is filled in automatically.

Step 3 Click **OK** to begin the authentication process.

Note If the password is invalid or entered incorrectly, the Token Configuration window reappears, enabling you to re-enter it.

If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

Using PEAP (EAP-MSCHAP V2)

After you (or auto profile selection) activate a profile that uses PEAP (EAP-MSCHAP V2) authentication or you eject and reinsert the client adapter, reboot the computer, or log on while this profile is active, the EAP authentication process begins automatically. The client adapter should EAP authenticate using either your Windows credentials or the username and password entered in the Define PEAP (EAP-MSCHAP V2) Configuration window.

If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

Restarting the Authentication Process

To force your client adapter to try to reauthenticate using the username and password of the current profile, choose **Reauthenticate** from the ASTU pop-up menu or the ADU Action drop-down menu. When you choose this option, the authentication process begins.

If your client adapter is unable to authenticate using the specified username and password, you may be prompted to re-enter them. If you click **Cancel**, a message appears indicating that the current profile will be disabled until you choose the Reauthenticate option, reboot your computer, or eject and reinsert the client adapter.

Viewing Status and Statistics

This chapter explains how to use ADU to view the client adapter's status and its transmit and receive statistics.

The following topics are covered in this chapter:

- Overview of ADU Status and Statistics Tools, page 7-2
- Setting Parameters that Affect ADU Status and Statistics Tools, page 7-2
- Viewing the Current Status of Your Client Adapter, page 7-4
- Viewing Statistics for Your Client Adapter, page 7-12

Overview of ADU Status and Statistics Tools

In addition to enabling you to configure your client adapter for use in various types of networks, ADU provides tools that enable you to assess the performance of the client adapter and other devices on the wireless network. These tools perform the following functions:

- Display your client adapter's current status and configured settings
- Display statistics pertaining to your client adapter's transmission and reception of data

Table 7-1 enables you to quickly find instructions for using ADU status and statistics tools.

Table 7-1 Status and Statistics Tool Instructions

Tool	Page Number
Status	7-4
Statistics	7-12

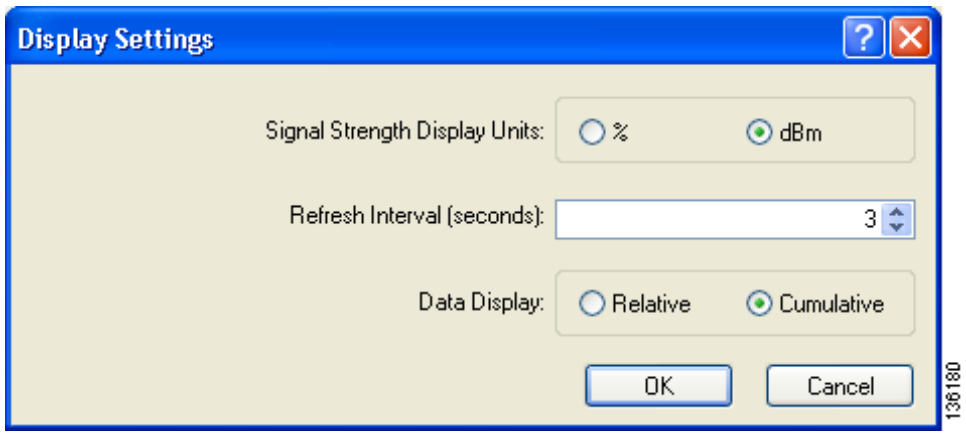
Setting Parameters that Affect ADU Status and Statistics Tools

Several parameters affect the operation of ADU status and statistics tools. Follow these steps to set these parameters.

Step 1 Open ADU.

Step 2 Choose **Display Settings** from the Options drop-down menu. The Display Settings window appears (see Figure 7-1).

Figure 7-1 Display Settings Window



Step 3 Table 7-2 lists and describes the parameters that affect the operation of ADU status and statistics tools. Follow the instructions in the table to change any parameters.

Table 7-2 Parameters Affecting ADU Status and Statistics Tools

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Signal Strength Display Units</td><td colspan="2">Specifies the units used to display signal strength on the Advanced Status window and signal-to-noise ratio (SNR) on the Available Infrastructure and Ad Hoc Networks window.
Options: % or dBm
Default: dBm</td></tr>
<tr><td></td><td>Units</td><td>Description</td></tr>
<tr><td></td><td>%</td><td>Displays the signal strength and signal-to-noise ratio as a percentage.</td></tr>
<tr><td></td><td>dBm</td><td>Displays the signal strength in decibels with respect to milliwatts (dBm) and the signal-to-noise ratio in decibels (dB).</td></tr>
<tr><td>Refresh Interval</td><td colspan="2">Specifies how often the ADU status and statistics windows and the ASTU icon are updated.
Range: 1 to 5 seconds between updates (in 1-second increments)
Default: 3 seconds between updates</td></tr>
<tr><td>Data Display</td><td colspan="2">Specifies whether the data that is displayed on the Diagnostics and Advanced Statistics windows continue to increment until the driver is reloaded or only until an update occurs (every 1 to 5 seconds).
Options: Relative or Cumulative
Default: Cumulative</td></tr>
<tr><td></td><td>Data Display</td><td>Description</td></tr>
<tr><td></td><td>Relative</td><td>Displays statistical data collected since the last update, as specified by the Refresh Interval (1 to 5 seconds).</td></tr>
<tr><td></td><td>Cumulative</td><td>Displays statistical data collected since the driver was loaded, upon card insertion or reboot.</td></tr>
</table>

Step 4 Click **OK** to save your changes.

Viewing the Current Status of Your Client Adapter

ADU enables you to view the current status of your client adapter as well as many of the settings that have been configured for the adapter. To view your client adapter's status and settings, open ADU. The Current Status window appears (see Figure 7-2).

Figure 7-2 Current Status Window

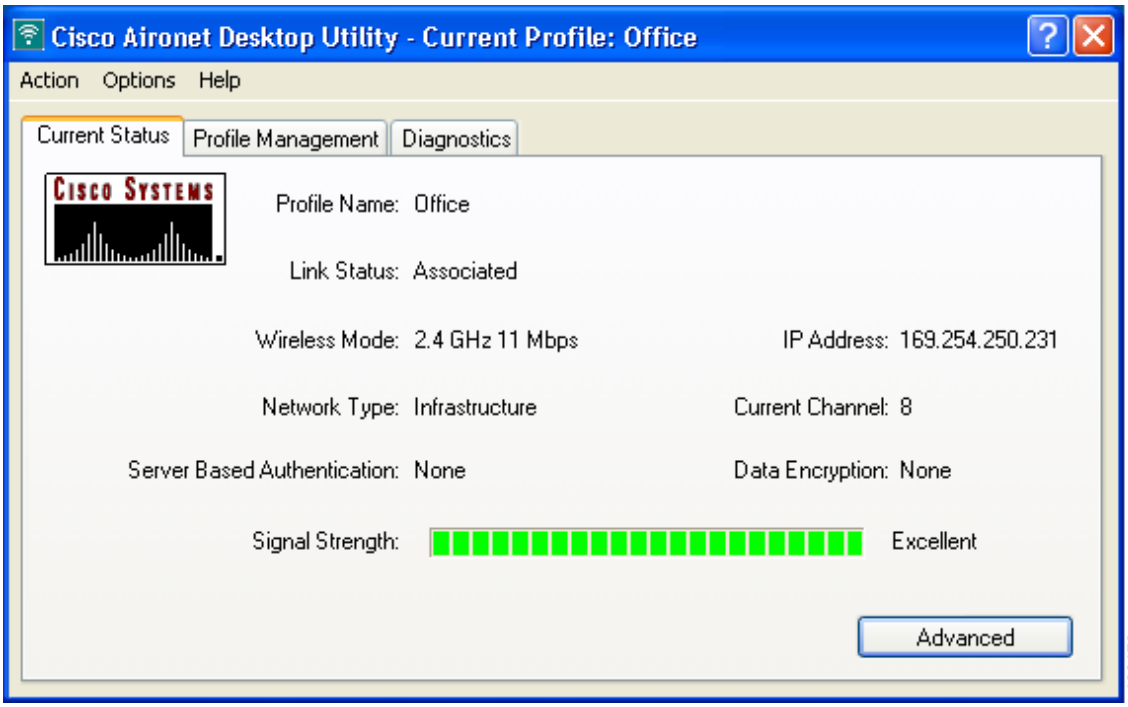


Table 7-3 interprets each element of the Current Status window.

Table 7-3 Basic Client Adapter Status

<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>Profile Name</td><td>The network configuration (or profile) your client adapter is currently using.
Note Refer to Chapter 4 for information on creating, modifying, and selecting profiles.</td></tr>
<tr><td>Link Status</td><td>The operational mode of your client adapter.
Value: Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, Authentication Failed Retrying
<table>
<tr><th>Link Status</th><th>Description</th></tr>
<tr><td>Not Associated</td><td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr>
<tr><td>Associated</td><td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr>
<tr><td>Authenticating</td><td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td></tr>
<tr><td>Authenticated</td><td>The client adapter is associated to an access point, and the user is EAP authenticated.</td></tr>
<tr><td>Authentication Failed</td><td>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</td></tr>
<tr><td>Authentication Failed Retrying</td><td>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</td></tr>
</table></td></tr>
<tr><td>Wireless Mode</td><td>The frequency and rate at which your current wireless connection is capable of transmitting or receiving packets.
Value: 5 GHz 54 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps
Note Refer to the Wireless Mode parameter in Table 5-3 for information on setting the wireless mode for your client adapter.</td></tr>
<tr><td>Network Type</td><td>The type of network in which your client adapter is being used.
Value: Infrastructure or Ad Hoc
Note Refer to the Network Type parameter in Table 5-3 for information on setting the network type.</td></tr>
</table>

Table 7-3 Basic Client Adapter Status (continued)

Status	Description
Server Based Authentication	The method by which authentication to a back-end server is being performed to establish secure connectivity. **Value:** None, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP **Note** Refer to the "Overview of Security Features" section on page 5-14 for details on these server-based authentication types.
IP Address	The IP address of your client adapter.
Current Channel	The channel that your client adapter is currently using for communications. This field displays *Scanning* while the client adapter searches for a channel. **Value:** Dependent on radio band and regulatory domain **Note** Refer to the Channel parameter in Table 5-3 for information on setting the channel for your client adapter. **Note** Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.
Data Encryption	The data encryption type that was negotiated with the access point (in infrastructure mode) or another client (in ad hoc mode) upon association. **Value:** None, WEP, CKIP, TKIP, or AES **Note** Refer to the "Overview of Security Features" section on page 5-14 for details on these data encryption types.
Signal Strength	The signal strength for all received packets. The color of this parameter's progress bar provides a visual interpretation of signal strength. **Value:** Excellent (green), Good (green), Fair (yellow), Poor (red), or No Link

Click **Advanced** if you want to view more detailed status information for your client adapter. The Advanced Status window appears (see Figure 7-3).

Figure 7-3 Advanced Status Window

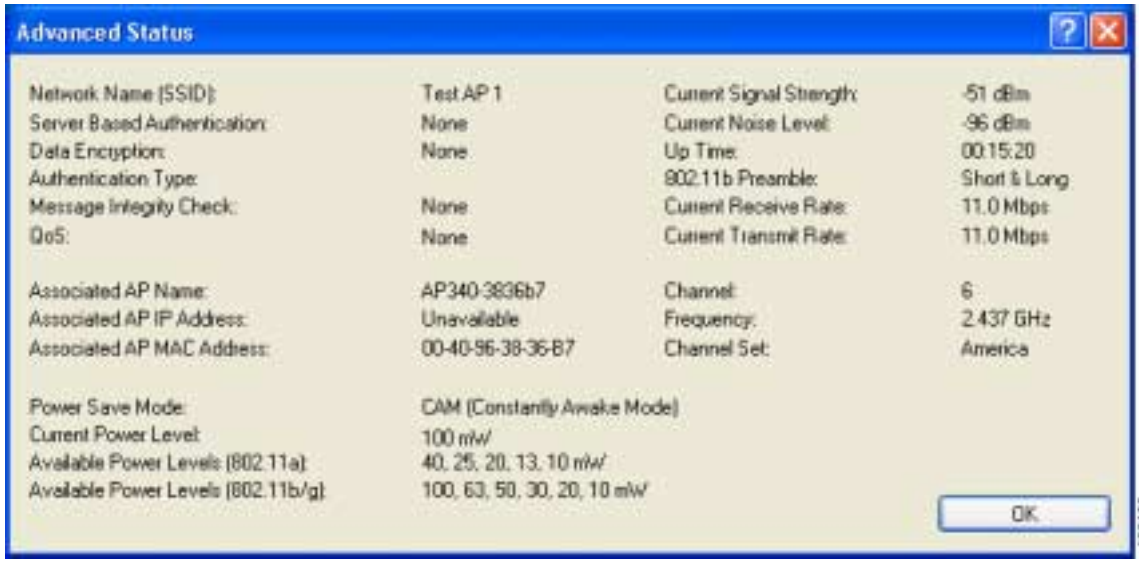


Table 7-4 interprets each element of the Advanced Status window.

Table 7-4 Advanced Client Adapter Status

Status	Description
Network Name (SSID)	The name of the network to which your client adapter is currently associated. **Note** Refer to the SSID1 parameter in Table 5-2 for information on setting the client adapter's SSID.
Server Based Authentication	The method by which authentication to a back-end server is being performed to establish secure connectivity. **Value:** None, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP Refer to the "Overview of Security Features" section on page 5-14 for details on these server-based authentication types.
Data Encryption	The data encryption type that was negotiated with the access point (in infrastructure mode) or another client (in ad hoc mode) upon association. **Value:** None, WEP, CKIP, TKIP, or AES **Note** Refer to the "Overview of Security Features" section on page 5-14 for details on these data encryption types.

Table 7-4 Advanced Client Adapter Status (continued)

Status	Description
Authentication Type	Specifies whether the client adapter must share the same WEP keys as the access point in order to authenticate or can authenticate to the access point regardless of its WEP settings. **Value:** Open or Shared **Note** An incorrect WEP key setting prevents connectivity to the network regardless of the 802.11 authentication type selected. **Note** Refer to the "Setting Advanced Parameters" section on page 5-6 for information on setting the 802.11 authentication mode.
Message Integrity Check	Indicates whether your client adapter is using message integrity check (MIC) to protect packets sent to and received from the access point. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. **Note** MIC is supported automatically by the client adapter's driver, but it must be enabled on the access point. **Value:** None, MMH, or Michael

Message Integrity Check	Description
None	MIC is disabled.
MMH	MIC is enabled and is being used with CKIP.
Michael	MIC is enabled and is being used with WPA and TKIP.

Table 7-4 Advanced Client Adapter Status (continued)

Status	Description
QoS	The type of quality of service that is currently being used by your client adapter. QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification. **Value:** None or WMM

QoS	Description
None	WMM standard QoS is not enabled.
WMM	Wi-Fi Multimedia, a component of the IEEE 802.11e WLAN standard for QoS, is enabled. For this value to appear, QoS and WMM must be enabled on the access point to which the client adapter is associated.

Note WMM is supported automatically on the client adapter in the software included in Install Wizard 2.0 or later. However, you must enable the Windows QoS Packet Scheduler to ensure WMM support. Follow the instructions in the "Enabling Wi-Fi Multimedia" section on page 5-51 to enable the QoS Packet Scheduler.

Associated AP Name	The name of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with a name, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). **Note** This field shows up to 15 characters although the name of the access point may be longer.
Associated AP IP Address	The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). **Note** If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.
Associated AP MAC Address	The MAC address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode. **Note** This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.

Table 7-4 Advanced Client Adapter Status (continued)

Status	Description
Power Save Mode	The client adapter's current power consumption setting. **Value:** CAM (Constantly Awake Mode), Max PSP (Max Power Saving), or Fast PSP (Power Save Mode) **Note** Refer to the Power Save Mode parameter in Table 5-3 for information on setting the client adapter's power save mode.
Current Power Level	The power level at which your client adapter is currently transmitting. The maximum level is dependent upon the radio band used and your country's regulatory agency. **Value:** 10, 13, 20, 25, or 40 mW (802.11a band); 10, 20, 30, 50, 63, or 100 mW (802.11b/g band) **Note** Refer to the Transmit Power Level parameter in Table 5-3 for information on setting the client adapter's power level.
Available Power Levels	The power levels at which your client adapter is capable of transmitting. The maximum level is dependent upon the radio band used and your country's regulatory agency. **Value:** 10, 13, 20, 25, or 40 mW (802.11a band); 10, 20, 30, 50, 63, or 100 mW (802.11b/g band) **Note** Refer to the Transmit Power Level parameter in Table 5-3 for information on the client adapter's available power levels.
Current Signal Strength	The signal strength for all received packets. The higher the value, the stronger the signal. **Range:** 0 to 100% or 0 to –100 dBm
Current Signal Quality	The signal quality for all received packets. The higher the value, the clearer the signal. **Range:** 0 to 100% **Note** This field appears only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.
Current Noise Level	The level of background radio frequency energy in the current radio band. The lower the value, the less background noise present. **Range:** 0 to –100 dBm **Note** This field appears only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in Table 7-2 for information.
Up Time	The amount of time (in hours:minutes:seconds) since the client adapter has been receiving power. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.

Table 7-4 Advanced Client Adapter Status (continued)

Status	Description
802.11b Preamble	Indicates whether your client adapter is using only long radio headers or short and long radio headers. **Value:** Short & Long or Long Only **Note** This field contains a value only when the client adapter is operated in 2.4-GHz 11-Mbps or 2.4-GHz 54-Mbps mode. **Note** Refer to the 802.11b Preamble parameter in Table 5-3 for information on using radio headers.
Current Receive Rate	The rate at which your client adapter is currently receiving data packets. **Value:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Current Transmit Rate	The rate at which your client adapter is currently transmitting data packets. **Value:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Channel	The channel that your client adapter is currently using for communications. This field displays *Scanning* while the client adapter searches for a channel. **Value:** Dependent on radio band and regulatory domain **Note** Refer to the Channel parameter in Table 5-3 for information on setting the channel for your client adapter. **Note** Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.
Frequency	The radio frequency that your client adapter is currently using for communications. This field displays *Scanning* while the client adapter searches for a frequency. **Value:** Dependent on radio band and regulatory domain **Note** Refer to the Wireless Mode parameter in Table 5-3 for information on setting the frequency for your client adapter.
Channel Set	The regulatory domain for which your client adapter is currently configured. This value is not user selectable. **Value:** America, EMEA, Japan, or Rest of World **Note** Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

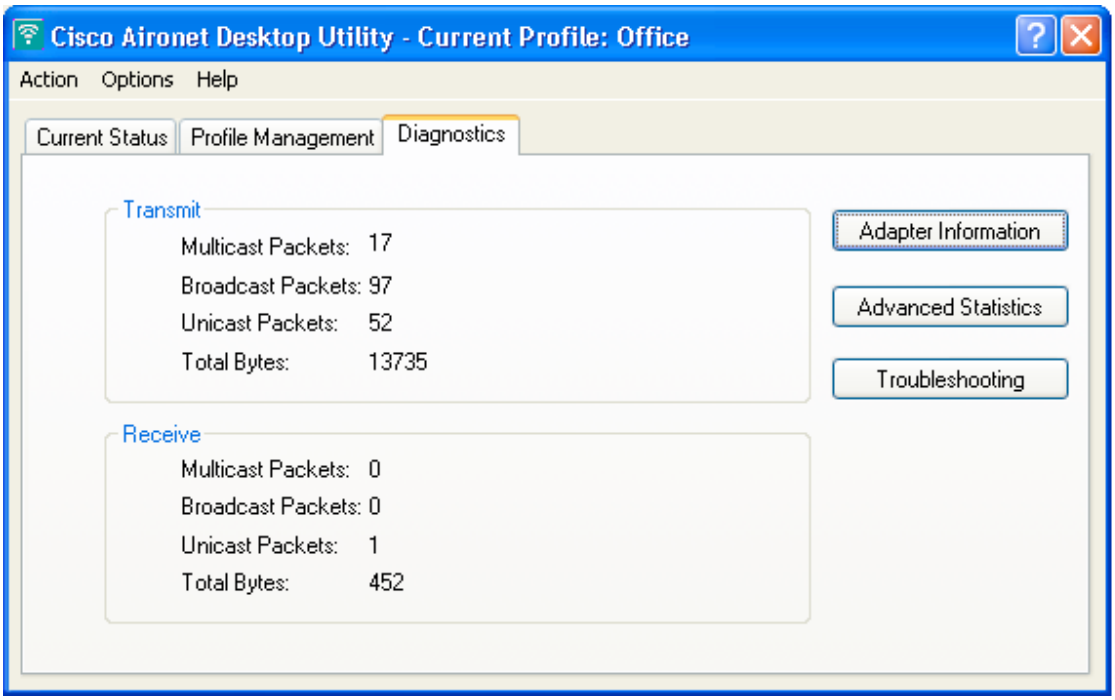
Click **OK** to close the Advanced Status window.

Viewing Statistics for Your Client Adapter

ADU enables you to view statistics that indicate how data is being received and transmitted by your client adapter.

To view your client adapter's statistics, open ADU and click the **Diagnostics** tab. The Cisco Aironet Desktop Utility (Diagnostics) window appears (see Figure 7-4).

Figure 7-4 Cisco Aironet Desktop Utility (Diagnostics) Window



This window displays basic transmit and receive statistics for your client adapter. The statistics are calculated on a relative or cumulative basis as specified by the Data Display parameter and are continually updated at the rate specified by the Refresh Interval parameter. Instructions for changing the Data Display and Refresh Interval settings are provided in Table 7-2.

Note The receive and transmit statistics are host statistics. That is, they show packets and errors received or sent by the Windows device.

Table 7-5 describes each statistic that is displayed for your client adapter.

Table 7-5 Basic Client Adapter Statistics

Statistic	Description
Transmit Statistics	
Multicast Packets	The number of multicast packets that were transmitted.
Broadcast Packets	The number of broadcast packets that were transmitted.
Unicast Packets	The number of unicast packets that were transmitted successfully.
Total Bytes	The number of bytes of data that were transmitted successfully.
Receive Statistics	
Multicast Packets	The number of multicast packets that were received.
Broadcast Packets	The number of broadcast packets that were received.
Unicast Packets	The number of unicast packets that were received successfully.
Total Bytes	The number of bytes of data that were received successfully.

Click **Advanced Statistics** if you want to view additional statistics for your client adapter. The Advanced Statistics window appears (see Figure 7-5).

Figure 7-5 Advanced Statistics Window

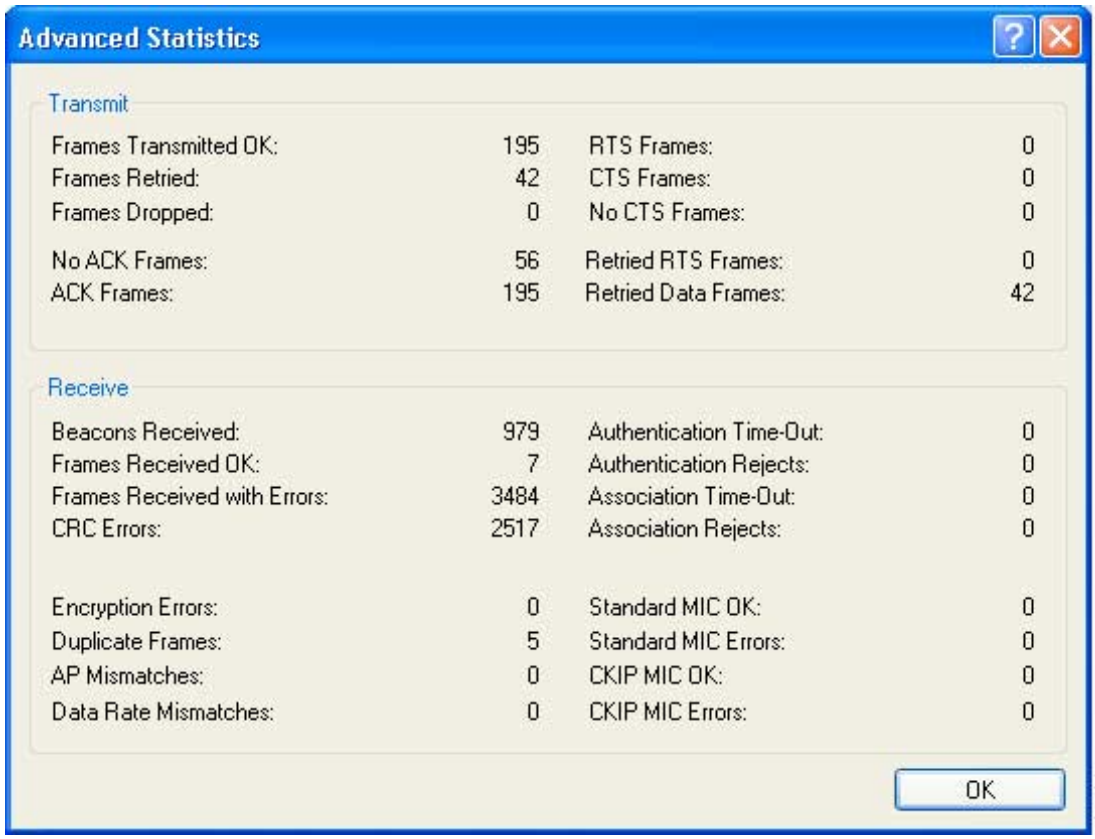


Table 7-6 interprets each element of the Advanced Statistics window.

Table 7-6 Advanced Client Adapter Statistics

Status	Description
Transmit Statistics	
Frames Transmitted OK	The number of frames that were transmitted successfully.
Frames Retried	The number of frames that were retried.
Frames Dropped	The number of frames that were dropped because of errors or collisions.
No ACK Frames	The number of transmitted frames that did not have their corresponding Ack frame received successfully.
ACK Frames	The number of transmitted frames that had their corresponding Ack frame received successfully.
RTS Frames	The number of request-to-send (RTS) transmissions that were attempted.
CTS Frames	The number of clear-to-send (CTS) frames that were received in response to a successfully transmitted RTS frame.
No CTS Frames	The number of request-to-send (RTS) transmissions that were unsuccessful. The access point sends CTS frames in response to the client's RTS frames. This field keeps track of each time the client does not receive a CTS back from the access point.
Retried RTS Frames	The number of request-to-send (RTS) frames that were retransmitted.
Retried Data Frames	The number of normal data frames that were retransmitted.
Receive Statistics	
Beacons Received	The number of beacon frames that were received successfully.
Frames Received OK	The number of all frames that were received successfully.
Frames Received with Errors	The number of frames that were received with an invalid checksum.
CRC Errors	The number of cyclic redundancy check (CRC) errors detected in the data portion of the frame.
Encryption Errors	The number of frames that were received with encryption errors.
Duplicate Frames	The number of duplicate frames that were received.
AP Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the access point was not the adapter's specified access point. **Note** Refer to the Access Point 1 through Access Point 4 parameters on page 5-13 for information on specifying access points.
Data Rate Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the adapter's data rate was not supported by the access point. **Note** Refer to the Wireless Mode parameter in Table 5-3 for information on supported data rates.

Table 7-6 Advanced Client Adapter Statistics (continued)

Status	Description
Authentication Time-Out	The number of times the client adapter tried to authenticate to an access point but was unable to because the access point did not respond fast enough (timed out).
Authentication Rejects	The number of times the client adapter tried to authenticate to an access point but was rejected.
Association Time-Out	The number of times the client adapter tried to associate to an access point but was unable to because the access point did not respond fast enough (timed out).
Association Rejects	The number of times the client adapter tried to associate to an access point but was rejected.
Standard MIC OK	The number of frames that were received with the correct message integrity check (MIC) value.
Standard MIC Errors	The number of frames that were discarded due to an incorrect message integrity check (MIC) value.
CKIP MIC OK	The number of frames that were received with the correct message integrity check (MIC) value when CKIP was being used. **Note** This field is displayed only if MIC is enabled on the access point.
CKIP MIC Errors	The number of frames that were discarded due to an incorrect message integrity check (MIC) value when CKIP was being used. **Note** This field is displayed only if MIC is enabled on the access point.

Click **OK** to close the Advanced Statistics window.

Using the Aironet System Tray Utility (ASTU)

This chapter explains how to use the Aironet System Tray Utility (ASTU) to access status information about your client adapter and perform basic tasks.

The following topics are covered in this chapter:

- Overview of ASTU, page 8-2
- The ASTU Icon, page 8-2
- Tool Tip Window, page 8-3
- Pop-Up Menu, page 8-5

Overview of ASTU

ASTU is an optional application that provides a small subset of the features available through ADU. Specifically, it enables you to access status information about your client adapter and perform basic tasks. ASTU is accessible from an icon in the Windows system tray, making it easily accessible and convenient to use. The ASTU icon appears only if a client adapter is installed in your computer and you did not disable ASTU during installation.

ASTU provides information and options in the following ways:

- In the appearance of the icon itself
- Through a tool tip window that appears when you hover the cursor over the icon
- Through a pop-up menu that appears when you right-click the icon
- Through a Connection Status window that appears when you double-click the icon

The ASTU Icon

The appearance of the ASTU icon indicates the connection status of your client adapter. ASTU reads the client adapter status and updates the icon every 1 to 5 seconds, depending on the value entered for the Refresh Interval on the Display Settings window. Table 8-1 interprets the different appearances of the ASTU icon.

Note Windows 2000 and XP may display their own wireless network connection status icon in the system tray. Cisco recommends that you turn off the Windows icon and use the ASTU icon to monitor your wireless connection.

Table 8-1 Interpreting the ASTU Icon

Icon	Description
	A white icon indicates that the client adapter's radio is disabled.
	A dark gray icon indicates that the client adapter is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode).
	A light gray icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode) but the user is not EAP authenticated.
	A green icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is excellent or good.

Table 8-1 Interpreting the ASTU Icon (continued)

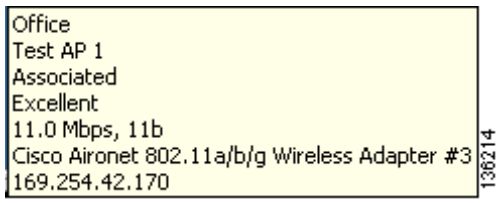
Icon	Description
	A yellow icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is fair.
	A red icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is poor.

Tool Tip Window

When you hover the cursor over the ASTU icon, the Tool Tip window appears (see Figure 8-1).

Note If the client adapter's radio is disabled, a message appears instead of the Tool Tip window to inform you that the wireless network interface is disabled.

Figure 8-1 Tool Tip Window



This window provides information on the current status of your client adapter. Table 8-2 lists and describes each element of the Tool Tip window.

Table 8-2 Tool Tip Window Elements

Status Element	Description
Active profile	The network configuration (or profile) that your client adapter is currently using. **Note** If auto profile selection is enabled, the active profile does not appear until the client is associated to an access point.
SSID	The name of the network to which your client adapter is currently associated. **Note** When the client adapter is not associated and auto profile selection is disabled, this field shows the profile's SSID. When the client adapter is not associated and auto profile selection is enabled, this field is left blank. **Note** Refer to the SSID1 parameter in Table 5-2 for information on setting the client adapter's SSID.

Table 8-2 Tool Tip Window Elements (continued)

<table>
<tr><th>Status Element</th><th>Description</th></tr>
<tr><td>Connection status</td><td>The operational mode of your client adapter.
Value: Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying

<table>
<tr><th>Connection Status</th><th>Description</th></tr>
<tr><td>Not Associated</td><td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr>
<tr><td>Associated</td><td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr>
<tr><td>Authenticating</td><td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td></tr>
<tr><td>Authenticated</td><td>The client adapter is associated to an access point, and the user is EAP authenticated.</td></tr>
<tr><td>Authentication Failed</td><td>The client adapter is associated to an access point, but the user has failed to EAP authenticate.
Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads Not Associated.</td></tr>
<tr><td>Authentication Failed Retrying</td><td>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.
Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads Not Associated.</td></tr>
</table>
</td></tr>
</table>

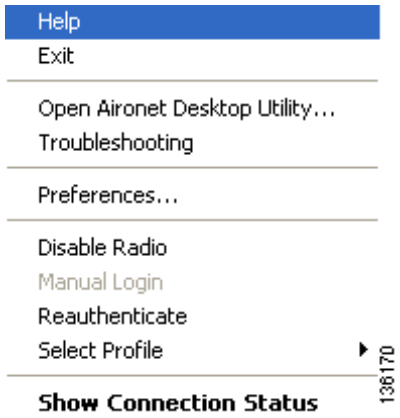
Table 8-2 Tool Tip Window Elements (continued)

Status Element	Description
Link quality	The client adapter's signal strength for all received packets. **Value:** Excellent, Good, Fair, Poor, or No Link
Link speed and 802.11 mode	The rate at which your client adapter is currently transmitting data packets and the 802.11 mode that your client adapter is currently using for communications. **Link speed value:**1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps **802.11 mode value:** 11a, 11b, or 11g
Client adapter type	A description of your client adapter.
Client adapter IP address	The IP address of your client adapter.

Pop-Up Menu

When you right-click the ASTU icon, the ASTU pop-up menu appears (see Figure 8-2).

Figure 8-2 ASTU Pop-Up Menu



The following sections describe each ASTU pop-up menu option.

Note If you used the Aironet System Tray Utility Preferences window or your system administrator used an administrative tool to deactivate certain ASTU menu options, these options do not appear in the menu and therefore cannot be selected.

Help

This option enables you to access the online help.

Exit

This option closes ADU and ASTU.

Note To reactivate ADU, double-click the **Aironet Desktop Utility** icon on your computer desktop. To reactivate ASTU, choose the **Enable Tray Icon** option from the ADU Action drop-down menu.

Open Aironet Desktop Utility

This option activates ADU.

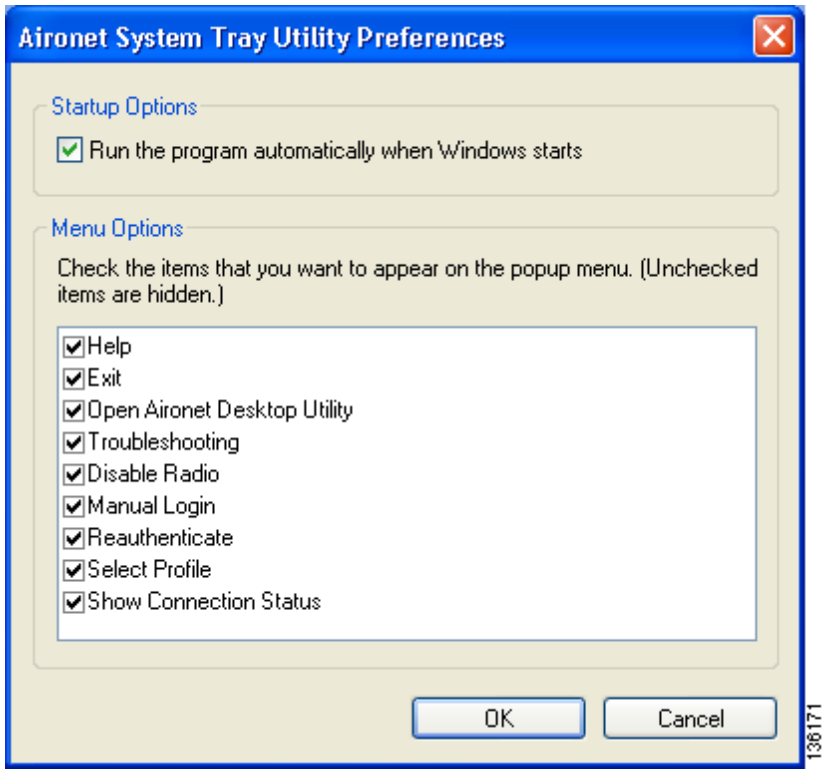
Troubleshooting

This option activates the troubleshooting utility, which enables you to identify and resolve configuration and association problems with your client adapter. Refer to the "Using the Troubleshooting Utility" section on page 10-3 for detailed instructions on using this utility.

Preferences

When you choose this option, the Aironet System Tray Utility Preferences window appears (see Figure 8-3).

Figure 8-3 Aironet System Tray Utility Preferences Window



This window enables you to determine when ADU and ASTU run and to choose the options that appear on the ASTU pop-up menu. Follow these steps to make your selections.

Step 1 If you want ASTU to run automatically when Windows starts, make sure the **Run the program automatically when Windows starts** check box is checked. Otherwise, uncheck this check box.

Note If you do not choose this option and later want to run ASTU, you must choose the **Enable Tray Icon** option from the Action drop-down menu in ADU.

Step 2 In the Menu Options portion of the window, make sure the check boxes of all the options that you want to appear in the ASTU pop-up menu are checked. Any options that are not checked will not be included in the menu.

Note The Preferences option cannot be deselected. It always appears in the ASTU pop-up menu.

Step 3 Click **OK** to save your changes.

Enable/Disable Radio

This option enables you to disable or enable the client adapter's radio. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You are using a laptop on an airplane and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is enabled, it periodically sends out probes even if it is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode), as required by the 802.11 specification. Therefore, it is important to disable it around devices that are susceptible to RF interference.

Note If the client adapter's radio is disabled, your client adapter is not associated, and a message appears when you hover the cursor over the ASTU icon to inform you that the wireless network interface is disabled.

Note If your client adapter's radio is disabled before your computer enters standby or hibernate mode or before you reboot the computer, the radio remains disabled when the computer resumes. You must enable the radio to resume operation.

If the radio is enabled, choose **Disable Radio** to disable the radio.

If the radio is disabled, choose **Enable Radio** to enable the radio.

Manual Login

This option enables you to manually invoke the authentication process for a profile that is configured to use a manually prompted LEAP or EAP-FAST username and password. When you choose this option, the Enter Wireless Network Password window appears. Enter your LEAP or EAP-FAST credentials and click **OK**. The LEAP or EAP-FAST Authentication Status window appears, and the authentication process begins.

Note Refer to Chapter 5 for information on setting a manual LEAP or EAP-FAST profile and Chapter 6 for details on the authentication process.

Reauthenticate

This option forces your client adapter to try to reauthenticate using the username and password of the current profile. It is available for all EAP-enabled profiles. When you choose this option, the authentication process begins.

If your client adapter is unable to authenticate using the specified username and password, you may be prompted to re-enter them. If you click **Cancel**, a message appears indicating that the current profile will be disabled until you choose the Reauthenticate option, reboot your computer, or eject and reinsert the client adapter.

Select Profile

This option enables you to select the active profile for your client adapter. When you choose this option, a profiles submenu appears (see Figure 8-4).

Figure 8-4 Profiles Submenu

From this menu, you can choose between the following options:

- **Use Auto Profile Selection**—Causes the client adapter's driver to automatically select a profile from the list of profiles that were set up in ADU to be included in auto profile selection.

  If the client adapter loses association for more than 10 seconds (or for more than the time specified by the LEAP/EAP-FAST authentication timeout value on the LEAP/EAP-FAST Settings window if LEAP/EAP-FAST is enabled), the driver switches automatically to another profile that is included in auto profile selection. The adapter will not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP/EAP-FAST authentication timeout value). To force the client adapter to associate to a different access point (in infrastructure mode) or another client (in ad hoc mode), you must select a new profile.

  Note This option is available only if two or more profiles are included in auto profile selection.

Note Login scripts are not reliable if you use auto profile selection with LEAP or EAP-FAST. If you authenticate and achieve full network connectivity before or at the same time as you log into the computer, the login scripts will run. However, if you authenticate and achieve full network connectivity after you log into the computer, the login scripts will not run.

- **A specific profile**—When you select a profile from the list of available profiles, the client adapter attempts to establish a connection to an access point (in infrastructure mode) or another client (in ad hoc mode) using the parameters that were configured for that profile.

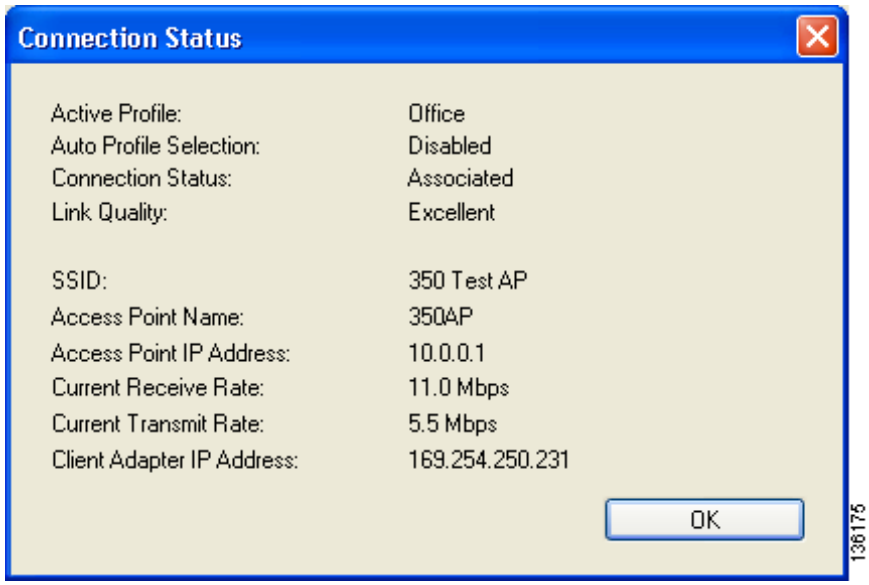
  If the client adapter cannot associate to the access point (or other client) or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To get it to associate, you must select a different profile or select Use Auto Profile Selection.

Simply click the desired profile to select it. A check mark appears beside the profile, and the client adapter attempts to establish a connection using the selected profile.

Show Connection Status

When you choose this option, the Connection Status window appears (see Figure 8-5).

Figure 8-5 Connection Status Window



This window provides information on the current status of your client adapter. Table 8-3 interprets each element of the Connection Status window.

Note You can also access the Connection Status window by double-clicking the ASTU icon.

Table 8-3 Connection Status Window Elements

<table>
<tr><th>Status Element</th><th>Description</th></tr>
<tr><td>Active Profile</td><td>The network configuration (or profile) that your client adapter is currently using.</td></tr>
<tr><td>Auto Profile Selection</td><td>Indicates whether your client adapter is using auto profile selection.
Value: Enabled or Disabled</td></tr>
<tr><td>Connection Status</td><td>The operational mode of your client adapter.
Value: Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying
<table>
<tr><th>Connection Status</th><th>Description</th></tr>
<tr><td>Not Associated</td><td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr>
<tr><td>Associated</td><td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr>
<tr><td>Authenticating</td><td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td></tr>
<tr><td>Authenticated</td><td>The client adapter is associated to an access point, and the user is EAP authenticated.</td></tr>
<tr><td>Authentication Failed</td><td>The client adapter is associated to an access point, but the user has failed to EAP authenticate.
Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads Not Associated.</td></tr>
<tr><td>Authentication Failed Retrying</td><td>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.
Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads Not Associated.</td></tr>
</table></td></tr>
</table>

Table 8-3 Connection Status Window Elements (continued)

Status Element	Description
Link Quality	The client adapter's signal strength for all received packets. **Value:** Excellent, Good, Fair, Poor, or No Link
SSID	The name of the network to which your client adapter is currently associated. **Note** Refer to the SSID1 parameter in Table 5-2 for information on setting the client adapter's SSID.
Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with a name, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). **Note** This field shows up to 15 characters although the name of the access point may be longer.
Access Point IP Address	The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). **Note** If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.
Current Receive Rate	The rate at which your client adapter is currently receiving data packets. **Value:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Current Transmit Rate	The rate at which your client adapter is currently transmitting data packets. **Value:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Client Adapter IP Address	The IP address of your client adapter.

Routine Procedures

This chapter provides procedures for common tasks related to the client adapter.

The following topics are covered in this chapter:

- Removing a Client Adapter, page 9-2
- Client Adapter Software Procedures, page 9-3
- Enabling or Disabling Your Client Adapter's Radio, page 9-9

Removing a Client Adapter

Follow the instructions in this section to remove a PC-Cardbus card or PCI card from a computing device, when necessary.

Caution These procedures and the physical connections they describe apply generally to conventional Cardbus slots and PCI expansion slots. In cases of custom or nonconventional equipment, be alert to possible differences in Cardbus slot and PCI expansion slot configurations.

Removing a PC-Cardbus Card

To remove a PC-Cardbus card after it is successfully installed and configured (such as when your laptop is to be transported), completely shut down your computer and pull the card directly out of the Cardbus slot. When the card is reinserted and the computer is rebooted, your connection to the network should be re-established.

Note If you need to remove your PC-Cardbus card but do not want to shut down your computer, double-click the **Unplug or Eject Hardware** icon in the Windows system tray, choose the Cisco Aironet client adapter you want to remove under Hardware devices, click **Stop**, and click **OK** to close each open window. Then pull the card directly out of the card slot.

Removing a PCI Card

Because PCI client adapters are installed inside desktop computers, which are not designed for portable use, you should have little reason to remove the adapter. However, instructions are provided below in case you need to remove your PCI card.

Step 1 Completely shut down your computer.

Step 2 Remove the computer cover.

Step 3 Remove the screw from the top of the CPU back panel above the PCI expansion slot that holds your client adapter.

Step 4 Pull up firmly on the client adapter to release it from the slot and carefully tilt the adapter to slip its antenna through the opening near the slot.

Step 5 Reinstall the screw on the CPU back panel and replace the computer cover.

Client Adapter Software Procedures

This section provides instructions for the following procedures:

- Upgrading the client adapter software, page 9-3
- Uninstalling the client adapter software, page 9-6
- ADU procedures, page 9-7
- ASTU procedures, page 9-9

Upgrading the Client Adapter Software

Follow these steps to upgrade your Cisco Aironet CB21AG or PI21AG client adapter software to a more recent release using the settings that were selected during the last installation.

Note If you want to upgrade your client adapter software using new installation settings, uninstall the previous installation (see the instructions on page 9-6); then install the new software (see the instructions on page 3-9).

Step 1 Make sure the client adapter is inserted in your computer.

Note If your client adapter is not inserted, the software cannot be upgraded.

Step 2 Use Windows Explorer to find the Install Wizard file.

Step 3 Double-click the file. The “Starting InstallShield Wizard” message appears followed by the Preparing Setup window (see Figure 9-1) and the Previous Installation Detected window (see Figure 9-2).

Figure 9-1 Preparing Setup Window

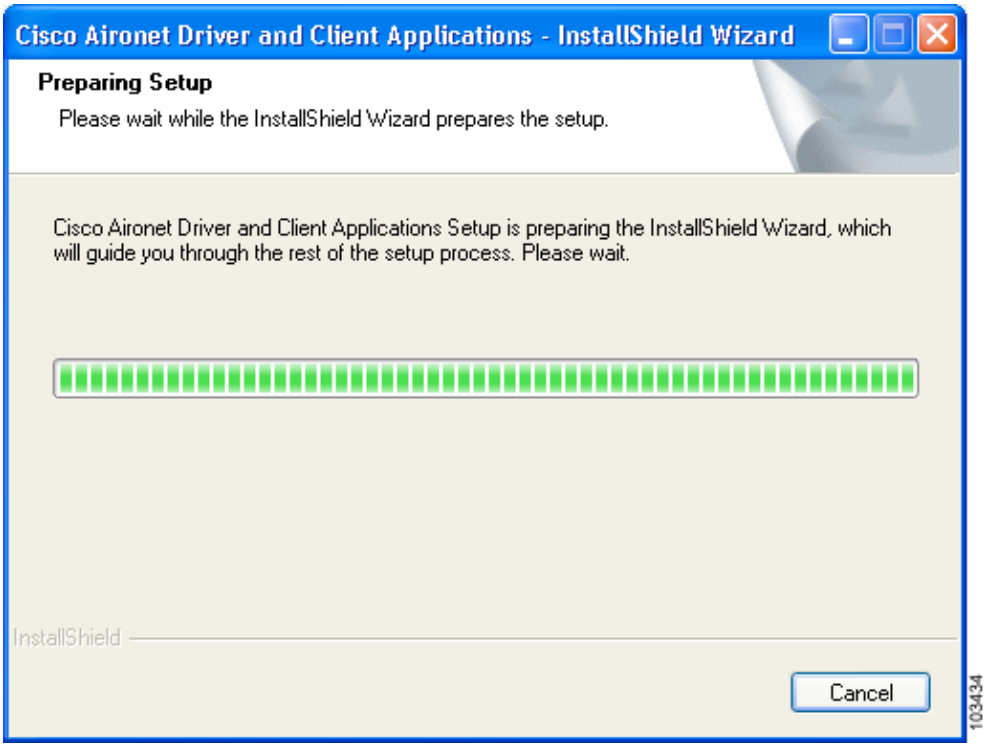
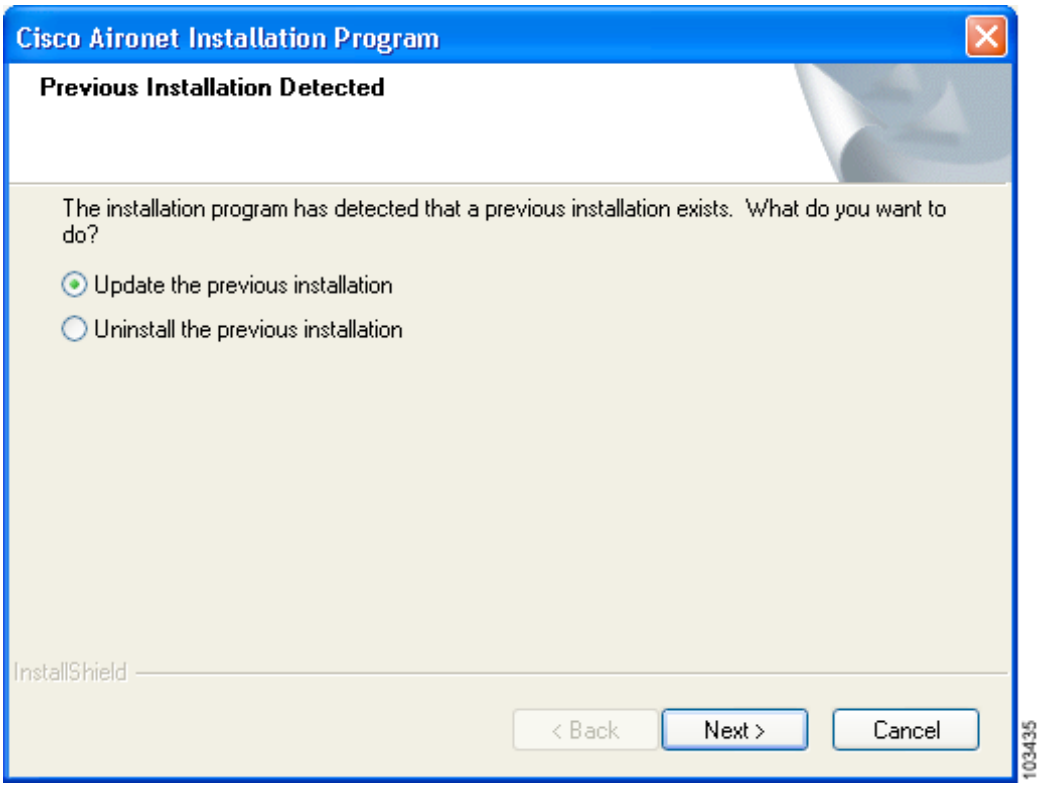


Figure 9-2 Previous Installation Detected Window



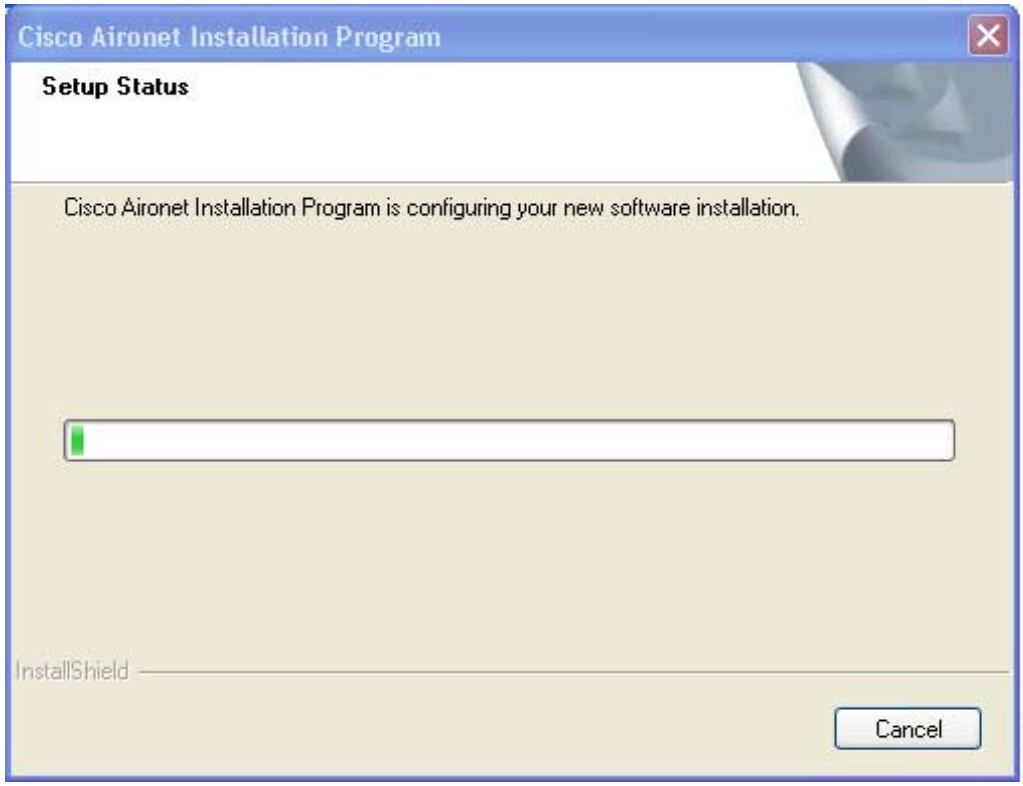
Step 4 Choose **Update the previous installation** and click **Next**.

Step 5 When a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.

Note If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.

The Setup Status window appears (see Figure 9-3).

Figure 9-3 Setup Status Window



The upgrade process begins, and you are notified as each software component is installed.

Step 6 When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart. The client adapter's software has been upgraded.

Uninstalling the Client Adapter Software

This section provides instructions for uninstalling the software for your Cisco Aironet CB21AG or PI21AG client adapter. This procedure is necessary if you want to remove installed client adapter software from your computer or downgrade to a previous release.

Note If you want to downgrade to an earlier release of client adapter software, use this procedure to uninstall the current software. Then install the older software.

Note When you uninstall the client adapter software, any existing profiles and stored PAC files are removed. If you want to save your profiles for later use, follow the instructions in Chapter 4 to export your profiles before uninstalling the software.

Step 1 Perform one of the following:

- If you want to remove the client adapter from your computer, shut down your computer, remove the client adapter, and reboot your computer. Then go to Step 2.
- If you want to leave your client adapter inserted in your computer, go to Step 2.

Step 2 Use Windows Explorer to find the Install Wizard file.

Note If you do not have the Install Wizard's setup.exe file, you can access the client adapter software by clicking **Control Panel** > **Add/Remove Programs** > **Cisco Aironet Installation Program** > **Remove**. Then follow the steps below beginning with the Preparing Setup window in Step 3.

Step 3 Double-click the file. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see Figure 9-1) and the Previous Installation Detected window (see Figure 9-2).

Step 4 Choose **Uninstall the previous installation** and click **Next**.

Step 5 When a message appears indicating that you are required to restart your computer at the end of the operation, click **Yes**. (If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.)

Step 6 When prompted to confirm your decision, click **OK**. The process to uninstall the files begins.

Step 7 When prompted to uninstall the device driver, click **Yes**.

Step 8 When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart.

Step 9 If you did not remove the client adapter from your computer, the Found New Hardware Wizard window appears after your computer reboots. Click **Cancel**. The client adapter software and its program folder have been uninstalled.

Note This procedure does not remove the Install Wizard file. If you want to remove it from your computer, find the file using Windows Explorer and delete it.

ADU Procedures

This section provides instructions for the following procedures:

- Opening ADU, page 9-7
- Exiting ADU, page 9-7
- Finding the version of ADU, page 9-8
- Viewing client adapter information, page 9-8
- Accessing online help, page 9-9

Opening ADU

To open ADU, perform one of the following:

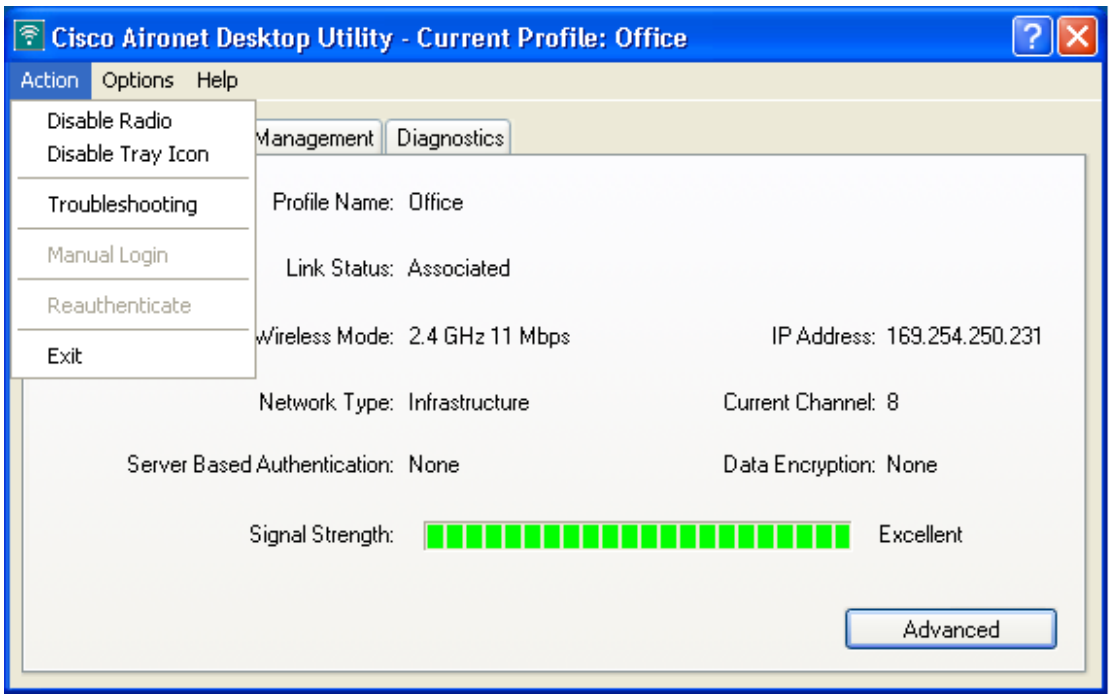
- Double-click the **Aironet Desktop Utility** icon on your desktop.
- Choose **Aironet Desktop Utility** from the folder in the Windows Start Menu that you chose during installation (the default location is **Start** > **Programs** > **Cisco Aironet** > **Aironet Desktop Utility**).
- Right-click the ASTU icon in the Windows system tray and choose **Open Aironet Desktop Utility**.

Exiting ADU

To exit ADU, perform one of the following:

- Choose **Exit** from the Action drop-down menu (see Figure 9-4).
- Right-click the ASTU icon in the Windows system tray and choose **Exit**.

Figure 9-4 Action Drop-Down Menu



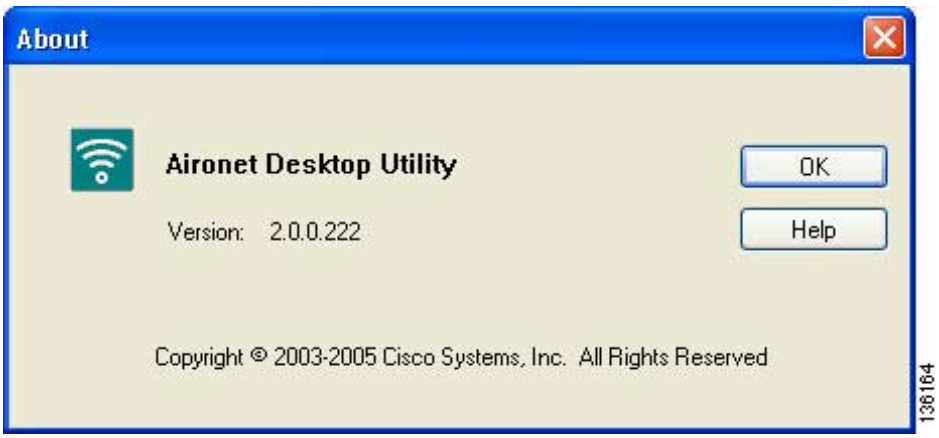
Finding the Version of ADU

Follow these steps to find the current version of ADU.

Step 1 Open ADU.

Step 2 Choose the **About Aironet Desktop Utility** option from the Help drop-down menu. The About window appears (see Figure 9-5).

Figure 9-5 About Window



Viewing Client Adapter Information

To view information about your client adapter, open ADU. Click the **Diagnostics** tab and **Adapter Information**. The Adapter Information window appears (see Figure 9-6).

Figure 9-6 Adapter Information Window

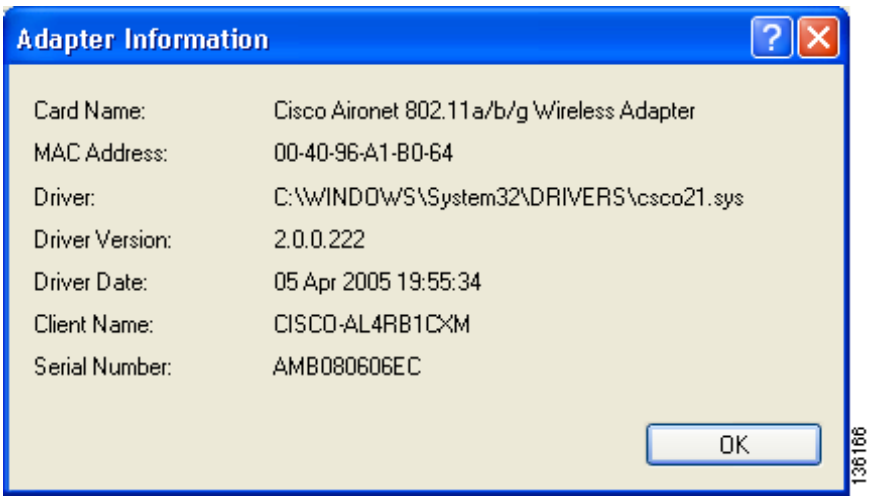


Table 9-1 interprets each element of the Adapter Information window.

Table 9-1 Adapter Information

Status	Description
Card Name	A description of your client adapter.
MAC Address	The MAC address assigned to your client adapter at the factory.
Driver	The filename and location of your client adapter's driver.
Driver Version	The version of the NDIS device driver that is currently installed on your computer.
Driver Date	The date that your client adapter's driver was created.
Client Name	The name your client adapter uses when it associates to an access point. **Note** Refer to the Client Name parameter in Table 5-2 for information on setting the client name.
Serial Number	The serial number of your client adapter.

Click **OK** to close the Adapter Information window.

Accessing Online Help

To access the ADU online help, open ADU. Then choose the **Aironet Desktop Utility Help** option from the Help drop-down menu.

ASTU Procedures

Refer to Chapter 8 for instructions on using ASTU.

Enabling or Disabling Your Client Adapter's Radio

Your client adapter's radio can be enabled or disabled. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You are using a laptop on an airplane and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is enabled, it periodically sends out probes even if it is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode), as required by the 802.11 specification. Therefore, it is important to disable it around devices that are susceptible to RF interference.

Note Your client adapter is not associated while its radio is disabled.

Note If your client adapter's radio is disabled before your computer enters standby or hibernate mode or before you reboot the computer, the radio remains disabled when the computer resumes. You must enable the radio to resume operation.

You can use ADU or ASTU to enable or disable the client adapter's radio. Follow the instructions below to use ADU or refer to the "Enable/Disable Radio" section on page 8-7 to use ASTU.

If your client adapter's radio is enabled, open ADU and choose **Disable Radio** from the Action drop-down menu (see Figure 9-4) to disable the radio.

If your client adapter's radio is disabled, open ADU and choose **Enable Radio** from the Action drop-down menu (see Figure 9-4) to enable the radio.

CHAPTER 10

Troubleshooting

This chapter provides information for diagnosing and correcting common problems that may occur when you install and operate the client adapter.

The following topics are covered in this chapter:

- Accessing the Latest Troubleshooting Information, page 10-2
- Interpreting the Indicator LEDs, page 10-2
- Troubleshooting the Client Adapter, page 10-3
- Error Messages, page 10-12

Accessing the Latest Troubleshooting Information

This chapter provides basic troubleshooting tips for your client adapter. For more up-to-date and detailed troubleshooting information, refer to the TAC web site. To access this site, go to Cisco.com, click **Technical Support** > **Product Support** > **Wireless**. Then choose your product and click **Troubleshooting** to find information on the problem you are experiencing.

Interpreting the Indicator LEDs

The client adapter shows messages through its two LEDs. Table 10-1 interprets the LED operating messages.

Table 10-1 LED Operating Messages

Status LED (green)	Activity LED (amber)	Condition
Off	Off	Client adapter is not receiving power.
Blinking slowly	Off	Client adapter is in power save mode.
On	Off	Client adapter has awakened from power save mode.
Alternating blink:		Client adapter is scanning for the wireless network for which it is configured.
On	Off	
Off	On	
Blinking slowly	Blinking slowly	Client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode).
Blinking quickly	Blinking quickly	Client adapter is transmitting or receiving data while associated to an access point (in infrastructure mode) or another client (in ad hoc mode).

Troubleshooting the Client Adapter

This section provides troubleshooting tips should you encounter problems with your client adapter. Use Table 10-2 to quickly find specific troubleshooting information.

Table 10-2 Troubleshooting Information

Troubleshooting Information	Page Number
Using the troubleshooting utility	10-3
Disabling the Microsoft Wireless Configuration Manager	10-8
Disabling the Microsoft 802.1X supplicant	10-8
Client adapter recognition problems	10-8
Resolving resource conflicts	10-9
Problems associating to an access point	10-10
Problems connecting to the network	10-11
Prioritizing network connections	10-11
Parameters missing from Profile Management windows	10-11
Windows Wireless Network Connection icon shows unavailable connection (Windows XP only)	10-11

Using the Troubleshooting Utility

The troubleshooting utility enables you to identify and resolve configuration and association problems with your client adapter. It is meant to be used only when the client adapter is in infrastructure mode because it assesses the connection between the adapter and an access point.

Follow the instructions in one of the subsections below to use the utility to diagnosis your client adapter's operation, save a detailed report to a text file, or access online help.

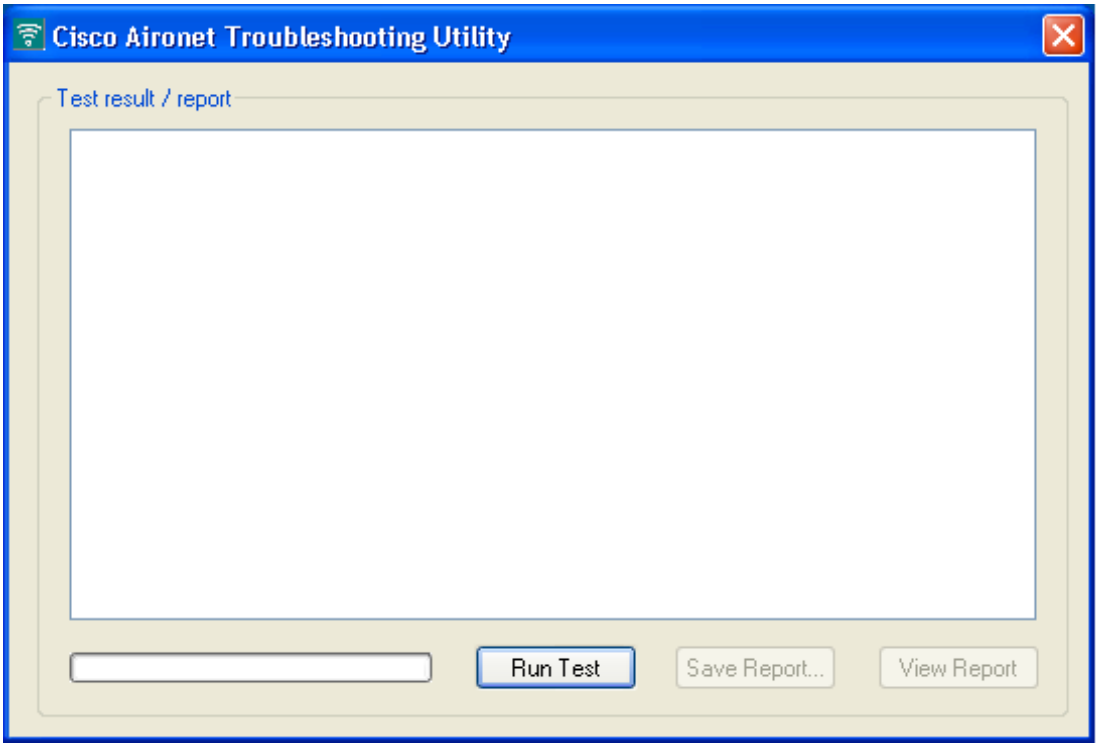
Diagnosing Your Client Adapter's Operation

Step 1 Perform one of the following to activate the troubleshooting utility:

- Open ADU; choose **Troubleshooting** from the Action drop-down menu.
- Open ADU; click the **Diagnostics** tab and **Troubleshooting**.
- Right-click the ASTU icon; choose **Troubleshooting** from the pop-up menu.

The Troubleshooting Utility window appears (see Figure 10-1).

Figure 10-1 Troubleshooting Utility Window

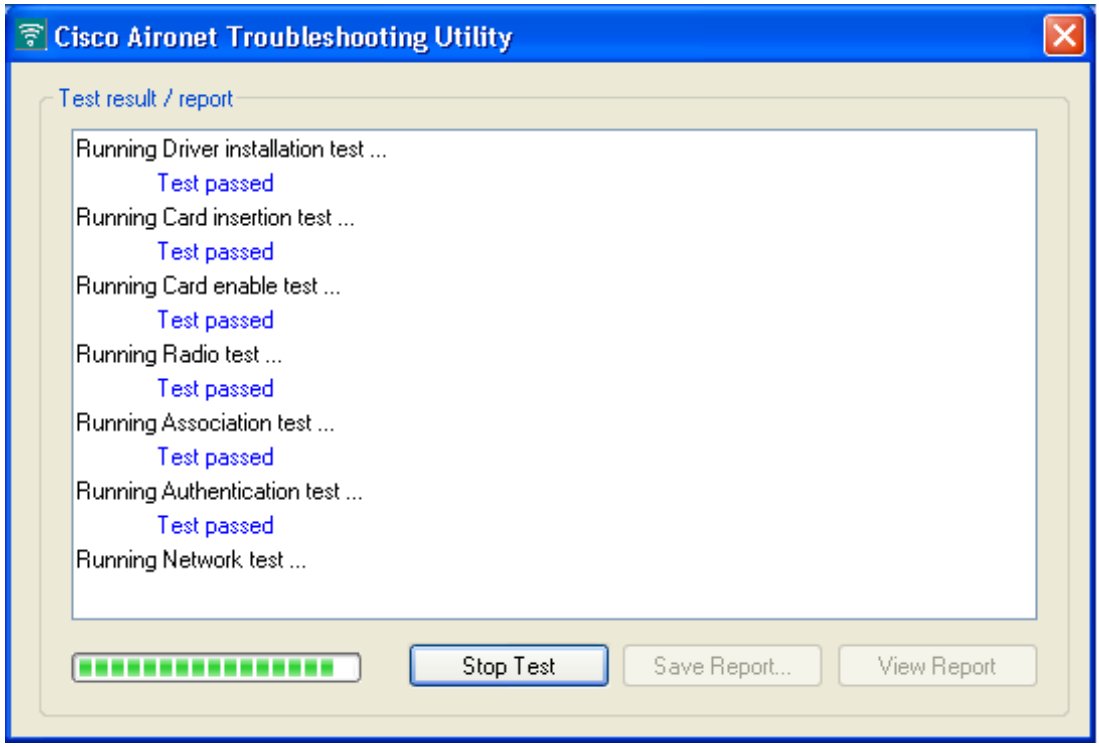


Step 2 Click **Run Test**. The utility performs the following series of seven tests to check the operation of your client adapter and to identify specific problems if they exist:

1. Driver installation test
2. Card insertion test
3. Card enable test
4. Radio test
5. Association test
6. Authentication test
7. Network test

The utility runs and then displays the results for each test (see Figure 10-2).

Figure 10-2 Troubleshooting Utility Window (with Test Results)



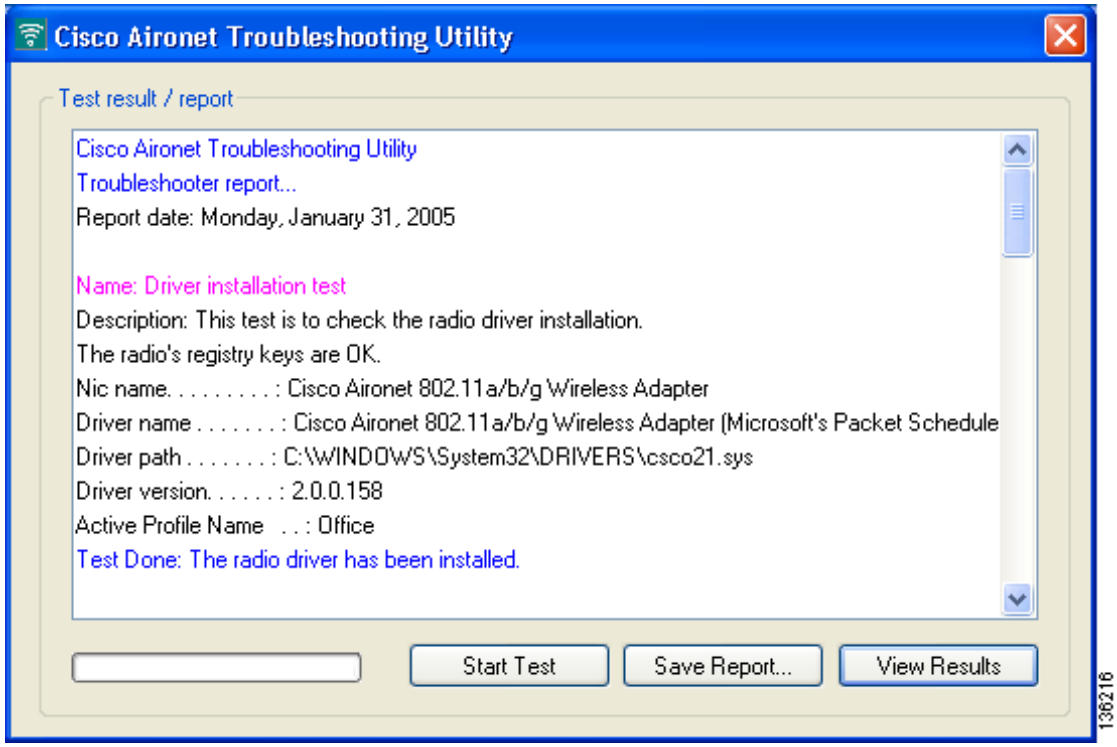
One of the following status messages appears for each test:

- **Test passed**—The test completed successfully.
- **Test bypassed**—The test was skipped because it was not required for the active profile.
- **Test failed**—The test failed. Follow the instructions in Step 3 to obtain more details.

Note You can click **Stop Test** at any time to stop the testing process, or you can click **Start Test** after the testing process has stopped to run the test again.

Step 3 To view more detailed information, click **View Report**. A report appears that provides more detailed results for your client adapter (see Figure 10-3).

Figure 10-3 Troubleshooting Utility Window (Detailed Report)



Note The report contains valuable information that, if necessary, could be used by your system administrator or TAC to analyze any problems. Follow the instructions in the next section if you want to save the report to a text file.

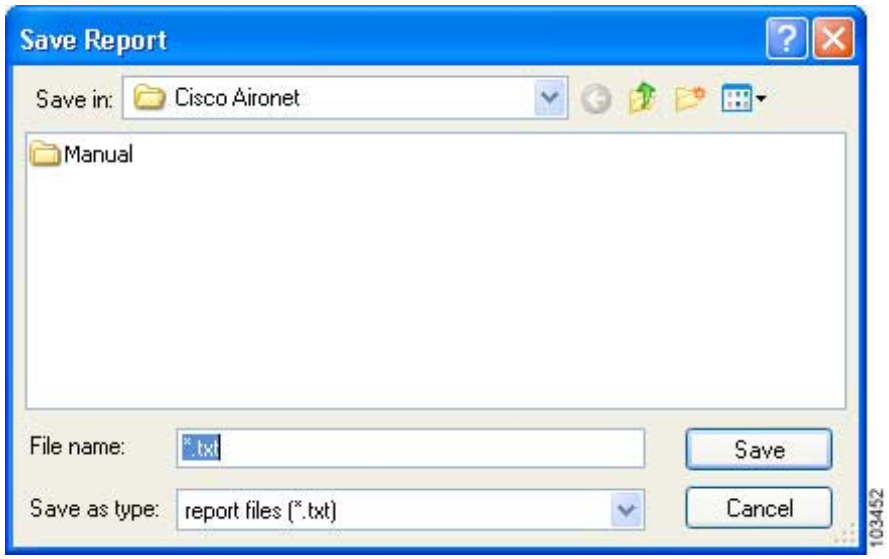
Step 4 If a problem is discovered, the report provides some possible repair suggestions. Follow the repair instructions carefully and run the troubleshooting utility again.

Saving the Detailed Report to a Text File

Follow the steps below to save the detailed troubleshooting report to your computer's hard drive.

Step 1 Click **Save Report**. The Save Report window appears (see Figure 10-4).

Figure 10-4 Save Report Window



Step 2 Enter a name for the detailed report in the File name field. The report is saved as a *.txt file.

Step 3 Use the Save in box at the top of the window to specify the location on your computer's hard drive where the file will be saved.

Note The default location is the directory where ADU is installed (such as C:\Program Files\Cisco Aironet).

Step 4 Click **Save**. The file is saved as a text file in the location specified.

Disabling the Microsoft Wireless Configuration Manager (Windows XP Only)

If any conflicts arise between ADU and the Microsoft Wireless Configuration Manager on a computer running Windows XP, follow these steps to disable the Microsoft configuration manager.

Note Disabling the Microsoft Wireless Configuration Manager on Windows XP also disables the Microsoft 802.1X supplicant. If you chose to configure your client adapter using ADU during installation, the Microsoft 802.1X supplicant should already be disabled.

Step 1 Double-click **My Computer**, **Control Panel**, and **Network Connections**.

Step 2 Right-click **Wireless Network Connection** and click **Properties**.

Step 3 Click the **Wireless Networks** tab and uncheck the **Use Windows to configure my wireless network settings** check box.

Step 4 Click **OK** to save your settings.

Disabling the Microsoft 802.1X Supplicant (Windows 2000 Only)

The Microsoft 802.1X supplicant can be installed on a computer running Windows 2000 through either a Microsoft hot fix or Windows 2000 Service Pack 4. If any conflicts arise between ADU and the Microsoft 802.1X supplicant, follow these steps to disable the Microsoft supplicant on a Windows 2000 computer.

Note The Microsoft 802.1X supplicant, if installed, should have been disabled during installation.

Step 1 Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**. Right-click **Local Area Connection**. Click **Properties**. The Local Area Connection Properties window appears.

Step 2 Click the **Authentication** tab.

Step 3 Uncheck the **Enable network access control using IEEE 802.1X** or **Enable IEEE 802.1x authentication for this network** check box.

Step 4 Click **OK** to save your settings.

Client Adapter Recognition Problems

If your computer's PCMCIA adapter does not recognize your client adapter, check your computer's BIOS and make sure that the PC card controller mode is set to PCIC compatible.

Note A computer's BIOS varies depending on the manufacturer. For support on BIOS-related issues, consult your computer's manufacturer.

Resolving Resource Conflicts

If you encounter problems while installing your client adapter on a computer running a Windows operating system, you may need to specify a different interrupt request (IRQ) or I/O range for the adapter.

The default IRQ for the client adapter is IRQ 10, which may not work for all systems. Follow the steps for your specific operating system to obtain an available IRQ.

During installation the adapter's driver installation script scans for an unused I/O range. The installation can fail if the I/O range found by the driver installation script is occupied by another device but not reported by Windows. An I/O range might not be reported if a device is physically present in the system but not enabled under Windows. Follow the steps for your specific operating system to obtain an available I/O range.

Resolving Resource Conflicts in Windows 2000

Step 1 Double-click **My Computer**, **Control Panel**, and **System**.

Step 2 Click the **Hardware** tab and **Device Manager**.

Step 3 Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.

Step 4 In the General window, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.

Step 5 Uncheck the **Use automatic settings** check box.

Step 6 Under Resource Settings or Resource Type, click **Input/Output Range**.

Step 7 Look in the Conflicting Device list at the bottom of the window. If it indicates that the range is being used by another device, click the **Change Setting** button.

Step 8 Scroll through the ranges in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the range is already being used.

Step 9 Click **OK**.

Step 10 Under Resource Settings or Resource Type, click **Interrupt Request**.

Step 11 Look in the Conflicting Device list at the bottom of the window. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.

Step 12 Scroll through the IRQs in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the IRQ is already being used.

Step 13 Click **OK**.

Step 14 Reboot your computer.

Resolving Resource Conflicts in Windows XP

Note These instructions assume you are using the Windows XP classic view, not the category view.

Step 1 Double-click **My Computer**, **Control Panel**, and **System**.

Step 2 Click the **Hardware** tab and **Device Manager**.

Step 3 Under Network Adapters, double-click the Cisco Systems Wireless LAN Adapter.

Step 4 In the General window, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.

Step 5 Uncheck the **Use automatic settings** check box.

Step 6 Under Resource Settings, click **I/O Range**.

Step 7 Look in the Conflicting Device list at the bottom of the window. If it indicates that the range is being used by another device, click the **Change Setting** button.

Step 8 Scroll through the ranges in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the range is already being used.

Step 9 Click **OK**.

Step 10 Under Resource Settings, click **IRQ**.

Step 11 Look in the Conflicting Device list at the bottom of the window. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.

Step 12 Scroll through the IRQs in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the IRQ is already being used.

Step 13 Click **OK**.

Step 14 Reboot your computer.

Problems Associating to an Access Point

Follow the instructions below if your client adapter fails to associate to an access point.

- If possible, move your workstation a few feet closer to an access point and try again.
- Make sure that the client adapter is securely inserted in your computer's client adapter slot.
- If you are using a PCI card, make sure that the antenna is securely attached.
- Make sure that the access point is turned on and operating.
- Check that all parameters are set properly for both the client adapter and the access point. These include the SSID, EAP authentication, WEP activation, network type, channel, etc.
- Follow the instructions in the previous section to resolve any resource conflicts.
- If the client adapter still fails to establish contact, refer to the "Obtaining Technical Assistance" section in the Preface for technical support information.

Problems Connecting to the Network

After you have installed the appropriate driver and client utilities, contact your IS department if you have a problem connecting to the network. Proxy server, network protocols, and further authentication information might be needed to connect to the network.

Prioritizing Network Connections

If your computer has more than one network adapter enabled (such as a Cisco Aironet client adapter and an Ethernet card), you can choose which one to use by assigning a priority to your network connections.

Follow the steps below to prioritize your network connections.

Step 1 Right-click the **My Network Places** icon on your desktop.

Step 2 Click **Properties**.

Step 3 Choose the **Advanced** menu option at the top of the window.

Step 4 Click **Advanced Settings**. Your network connections are listed in the Connections box on the Adapters and Bindings tab.

Step 5 Use the arrows beside the Connections box to move the network connection that you want to use to the top.

Step 6 Click **OK**.

Parameters Missing from Profile Management Windows

If some parameters are unavailable on the Profile Management windows, your system administrator may have used an administrative tool to deactivate these parameters. In this case, these parameters cannot be selected.

Windows Wireless Network Connection Icon Shows Unavailable Connection (Windows XP Only)

If your computer is running Windows XP and you configured your client adapter using ADU, the Windows Wireless Network Connection icon in the Windows system tray may be marked with a red *X* and show an unavailable connection even though a wireless connection exists. This is caused by a conflict between the wireless network settings of ADU and Windows XP. Simply ignore the Windows icon and use the ASTU icon to check the status of your client adapter's wireless connection.

Error Messages

This section provides a list of error messages that may appear during the installation, configuration, or use of your client adapter. The messages are listed in alphabetical order within each section, and an explanation as well as a recommended user action are provided for each message.

Error Message `ADU can hold only 16 profiles. To add another profile, either delete an existing profile or modify an existing profile.`

Explanation You attempted to create a new profile, import a profile, or activate a profile from the scan list on the Available Infrastructure and Ad Hoc Networks window after the maximum number of profiles had already been reached.

Recommended Action Modify an existing profile or delete a profile and then create a new one.

Error Message `Are you sure you want to delete this PAC from your local system? You might not be able to authenticate with the EAP-FAST profiles that use this PAC once the PAC is deleted.`

Explanation You are about to delete a PAC from either the Global or Private PAC store.

Recommended Action If you want to delete the PAC, click **Yes**. Otherwise, click **No**.

Error Message `At least one wireless checkbox must be selected.`

Explanation You clicked **OK** or selected another Profile Management tab before selecting any Wireless Mode options on the Profile Management (Advanced) window.

Recommended Action Choose at least one of the Wireless Mode options.

Error Message `Authentication failed.`

Explanation The domain logon failed for an unknown reason.

Recommended Action Try again to authenticate. If this message reappears, verify that all of the proper certificates have been loaded onto your computer and that your client adapter's current profile has been configured properly. If the domain logon continues to fail, contact your system administrator.

Error Message `Authentication failed because server rejected username or password.`

Explanation The domain logon failed because your username or password is invalid.

Recommended Action Re-enter your username and password on the Define PEAP (EAP-GTC) Configuration window or the Define PEAP (EAP-MSCHAP V2) Configuration window and save your settings. Then try again to authenticate.

Error Message `Authentication failed due to invalid client attributes (e.g., Login Name).`

Explanation The domain logon failed because of an invalid client configuration setting, such as a mistyped login name.

Recommended Action Return to the PEAP configuration windows, verify your settings, and make any necessary modifications.

Error Message `Authentication failed due to invalid client certificate.`

Explanation The domain logon failed because of an invalid client certificate.

Recommended Action Contact your system administrator to obtain a valid certificate.

Error Message `Authentication failed due to invalid server certificate.`

Explanation The domain logon failed because of an invalid server certificate.

Recommended Action Contact your system administrator.

Error Message `Authentication failed due to invalid server/domain name.`

Explanation The domain logon failed because of an invalid server/domain name.

Recommended Action Make sure the Specific Server or Domain field is blank on the Advanced Configuration window for PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2). Then follow the instructions in the "Enabling PEAP (EAP-GTC)" section on page 5-42 or the "Enabling PEAP (EAP-MSCHAP V2) Machine Authentication with Machine Credentials" section on page 5-49 to correctly enter your username in the Login Name field.

Error Message `Authentication timed out. Do you want to retry?`

Explanation LEAP or EAP-FAST authentication failed because the authentication server is down.

Recommended Action Click **Retry** to try to authenticate again using the same credentials or click **Cancel** to cancel the operation.

Error Message `Cannot load oemres.dll.`

Explanation The oemres.dll file cannot be installed.

Recommended Action Uninstall the current client adapter software; then install the latest release.

Error Message `Cisco Aironet 802.11a/b/g wireless adapter software update can't proceed. Please insert the adapter in the system and try again.`

Explanation You attempted to upgrade your client adapter's software when the adapter was not inserted in your computer.

Recommended Action Click **OK**, insert your client adapter, and start the upgrade process again.

Error Message `DHCP failure.`

Explanation The domain logon failed because of a DHCP failure.

Recommended Action Try again to authenticate. If this message reappears, contact your system administrator.

Error Message `During installation, you chose not to use Microsoft Wireless Configuration Manager to control your Cisco Aironet Wireless LAN Client Adapter. However, it is currently enabled for this device. Do you want to disable it?`

Explanation The Microsoft Wireless Configuration Manager is enabled and can be used to control your client adapter.

Recommended Action If you want to switch control from the Microsoft Wireless Configuration Manager to ADU, click **Yes**. Otherwise, click **No**.

Error Message `Entry must be` *`xx`* `characters long. Please enter` *`xx`* `more characters.`

Explanation The static WEP key that you entered on the Define Pre-Shared Keys window does not contain the correct number of characters.

Recommended Action Re-enter the static WEP key following the guidelines in the "Enabling Static WEP" section on page 5-24.

Error Message `Error importing the EAP-FAST PAC file.`

Explanation An error occurred while a PAC file was being imported. The operation was not completed.

Recommended Action Try again to import the PAC file. If the same message appears, obtain a new PAC file from your system administrator and import it.

Error Message `Failed to initialize supplicant. This error may be due to the absence of a valid machine certificate or the incomplete configuration of profiles.`

Explanation The domain logon failed because the EAP supplicant could not be initialized.

Recommended Action Verify that a valid machine certificate has been loaded onto your computer and that your client adapter's current profile has been configured properly.

Error Message `Failed to open PAC stores.`

Explanation An error occurred when you attempted to access the global or private PAC store.

Recommended Action Try again. If the second attempt fails, contact your system administrator.

Error Message `In order to select an Ad Hoc network, you must have a Network Name. Do you want to enter a Network Name?`

Explanation You chose Ad Hoc for Network Type on the Profile Management (Advanced) window, but a network name was not entered on the Profile Management (General) window.

Recommended Action If you want to set up an ad hoc network, click **Yes** and enter a network name in the SSID1 field on the Profile Management (General) window. Otherwise, click **No**.

Error Message `Invalid profile data. Please enter valid profile data.`

Explanation You improperly configured a profile (for example, you set up the profile to use EAP-TLS authentication, but no certificates are installed on your computer).

Recommended Action Modify the profile's configuration settings.

Error Message `Make sure the same new password is entered twice.`

Explanation You did not enter the same EAP-FAST password in both the New Password and Verify New Password fields on the Please Change Password window.

Recommended Action Carefully re-enter your new EAP-FAST password in both the New Password and Verify New Password fields on the Please Change Password window.

Error Message `No user certificates were found on your computer. Machine certificates will be used for Domain Logon if "Use Machine Information For Domain Logon" check box is checked.`

Explanation You chose the EAP-TLS option on the Profile Management (Security) window, but no user certificates were found on your computer.

Recommended Action Perform one of the following:

- If you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials, check the **Use Machine Information For Domain Logon** check box when the Define Certificate window appears.
- If you want the client to authenticate using user credentials, install the appropriate user certificate on your computer.

Error Message `Please enter a Passphrase.`

Explanation You clicked **OK** on the Define WPA/WPA2 Pre-Shared Key window before entering a Passphrase.

Recommended Action Enter a WPA/WPA2 Passphrase on the Define WPA/WPA2 Pre-Shared Key window and then click **OK**.

Error Message `Please enter a profile name.`

Explanation While creating a new profile, you clicked **OK** or chose another Profile Management tab before entering a profile name on the Profile Management (General) window.

Recommended Action Enter a profile name.

Error Message `Please enter at least one shared key.`

Explanation You clicked **OK** on the Define Pre-Shared Keys window before entering a static WEP key.

Recommended Action Enter at least one static WEP key on the Define Pre-Shared Keys window.

Error Message `Please enter exactly 12 characters, or leave the entry field empty.`

Explanation You entered fewer than 12 characters in one of the fields on the Preferred Access Points window.

Recommended Action Leave the fields on the Preferred Access Points window empty or re-enter the MAC address for the specified access point, which must be exactly 12 characters.

Error Message `The configuration name you entered is already being used. Enter a unique name.`

Explanation While creating a new profile, you entered a profile name on the Profile Management (General) window that already exists.

Recommended Action Enter a new profile name.

Error Message `The current EAP-FAST profile does not have a PAC or the configured PAC does not match the authentication server. Do you want to use another PAC found on your local system that matches the authentication server without reconfiguring the current EAP-FAST profile?`

Explanation The client adapter's authentication attempt failed because a valid PAC was not found. ADU matches the username and server name that it is trying to use with those in the PAC. If they do not match or the configured PAC does not exist, ADU searches the private and global stores. If a matching PAC is found, the user is prompted with this message before the PAC is used.

Recommended Action Click **Yes** to attempt to authenticate using another PAC on your system without having to reconfigure your profile.

Error Message `The EAP-FAST auto provisioning or PAC updating failed. The current profile is disabled until you correct the PAC configuration in the profile and reauthenticate.`

Explanation PAC provisioning has failed. No PAC has been provisioned, and the profile is disabled.

Recommended Action Try again to authenticate using the existing profile. If automatic PAC provisioning is enabled, make sure to allow a PAC to be provisioned if prompted. If the authentication attempt fails again, modify the profile's PAC configuration settings.

Error Message `The entered password was incorrect. Please try again.`

Explanation You incorrectly entered the PAC file password.

Recommended Action Carefully re-enter the PAC file password.

Error Message `The imported PAC already exists on your local machine. Do you want to update it anyway?`

Explanation You tried to import a PAC file with the same PAC ID as a previously imported PAC file.

Recommended Action Click **Yes** to replace the existing PAC with the new one from the imported file or click **No** to cancel the operation.

Error Message `The new password must be different from the old password.`

Explanation You entered your old EAP-FAST password in the New Password and/or Verify New Password fields on the Please Change Password window.

Recommended Action Enter your new EAP-FAST password in the New Password and/or Verify New Password fields on the Please Change Password window.

Error Message `The Passphrase must be between 8 and 64 characters.`

Explanation The WPA/WPA2 Passphrase that you entered on the Define WPA/WPA2 Pre-Shared Key window did not contain the correct number of characters.

Recommended Action Enter a WPA/WPA2 Passphrase with 8 to 63 ASCII text characters or 64 hexadecimal characters.

Error Message `The password is empty. Please enter a password.`

Explanation You chose the Use Saved User Name and Password option on the LEAP or EAP-FAST Settings window but did not enter a password, or you did not enter a password on the Enter Wireless Network Password window.

Recommended Action Enter your LEAP or EAP-FAST password in the Password field.

Error Message `The passwords you entered do not match. Please enter them again.`

Explanation The passwords that you entered in the Password and Confirm Password fields on the LEAP or EAP-FAST Settings window do not match.

Recommended Action Re-enter your LEAP or EAP-FAST password in both fields.

Error Message `The profile will be disabled until you select the Reauthentication option, Windows restarts, or the card is ejected and reinserted. Are you sure?`

Explanation The username and password for your current profile have expired or are no longer valid. When the Enter Network Password window appeared, prompting you to enter your new username and password, you chose Cancel. The profile was disabled to prevent accidental authentication attempts in the future.

Recommended Action Click **No**, enter your username and password when the Enter Wireless Network Password window reappears, and click **OK**. The client adapter should authenticate using your new credentials. If the profile uses saved credentials, edit the profile in ADU by changing the username and password on the LEAP or EAP-FAST Settings window and save your changes. (If you click **Yes**, the profile is disabled until you choose Reauthenticate from ASTU or the Action drop-down menu in ADU, reboot your system, or eject and reinsert the card.)

Error Message `The specified path does not exist. Please enter another path.`

Explanation You chose the **Make Driver Installation Diskette(s)** option during installation, but a diskette was not inserted in the computer's A: drive.

Recommended Action Insert a floppy diskette into your computer's floppy disk drive, and choose the **Make Driver Installation Diskette(s)** option again.

Error Message `The user name is empty. Please enter a user name.`

Explanation You chose the Use Saved User Name and Password option on the LEAP or EAP-FAST Settings window but did not enter a username, or you did not enter a username on the Enter Wireless Network Password window.

Recommended Action Enter your LEAP or EAP-FAST username in the User Name field.

Error Message `This Device is controlled by the Windows XP Automatic Wireless Network Configuration. It may override Network Name, Security and other settings from this profile.`

Explanation You attempted to activate ADU while the Microsoft Wireless Configuration Manager in Windows XP was enabled. When a message appeared asking if you wanted to disable the Microsoft configuration manager, you chose No.

Recommended Action If you want to use ADU to configure your client adapter, disable the Microsoft Wireless Configuration Manager.

Error Message `This Product does not support this version of Windows. Please check the product documentation for the system requirements.`

Explanation You tried to install the CB21AG and PI21AG client adapter software on an unsupported Windows operating system.

Recommended Action Install the CB21AG and PI21AG client adapter software on a computer running Windows 2000 or XP.

Error Message `Unable to authenticate wireless user. Please make sure you have entered the right user name and password and try again. If you are using an old PAC with this profile and have not logged on to the network for a long period of time, you may also want to make sure the PAC you are using is not expired by either import a new PAC manually or delete the old PAC if auto provisioning is enabled.`

Explanation The client adapter's authentication attempt failed either because the wrong user credentials were entered or the profile is using an old PAC.

Recommended Action Try to authenticate again using the existing profile. Make sure to enter your username and password correctly. If the authentication attempt fails again, import a new PAC or delete the old PAC is automatic PAC provisioning is enabled.

Error Message `Unable to copy PAC data. Make sure you have access rights.`

Explanation Your attempt to copy a PAC from the private store to the global store failed. You may not have the necessary permissions.

Recommended Action Try again. If your second attempt fails, contact your system administrator.

Error Message `Unable to delete the PAC from the local system.`

Explanation Your attempt to delete a PAC failed.

Recommended Action Try again. If your second attempt fails, contact your system administrator.

Error Message `Unable to EAP-FAST authenticate the wireless user in the specified amount of time. Network infrastructure might be down. You may also want to increase the timeout value for this profile.`

Explanation The client adapter was unable to EAP-FAST authenticate within the amount of time specified by the EAP-FAST authentication timeout value.

Recommended Action Try again to authenticate using the existing profile. If automatic PAC provisioning is enabled, make sure to allow a PAC to be provisioned if prompted. If the authentication attempt fails again, increase the authentication timeout value on the EAP-FAST Settings window and try again.

Error Message `Unable to save imported PAC data. Access denied.`

Explanation Your attempt to save an imported PAC file has failed. You may not have the necessary permissions.

Recommended Action Try again. If your second attempt fails, contact your system administrator.

Error Message `WEP Key x must be y characters long. Please enter z more characters.`

Explanation You entered an incomplete static WEP key on the Define Pre-Shared Keys window and clicked **OK**.

Recommended Action Re-enter the static WEP key, making sure to enter the correct number of characters and click **OK**.

Error Message `'x' contains characters which are non-hexadecimal.`

Explanation One of the static WEP keys on the Define Pre-Shared Keys window contains non-hexadecimal characters even though Hexadecimal is specified as the Key Entry type.

Recommended Action Re-enter the static WEP key following the guidelines in the "Enabling Static WEP" section on page 5-24.

Error Message `'x' is not a hexadecimal character.`

Explanation The character you entered on the Define Pre-Shared Keys window is not a hexadecimal character.

Recommended Action Re-enter the static WEP key following the guidelines in the "Enabling Static WEP" section on page 5-24.

Error Message `You are not registered with the authentication server. A security credential is required to register this device. Do you want to obtain a security credential?`

Explanation Automatic PAC provisioning is enabled for this profile. However, a valid PAC matching the server to which the client adapter is connecting could not be found.

Recommended Action Click **Yes** to provision a new PAC for this server using your existing credentials or click **No** to cancel the operation. If you click No, the client adapter is unable to authenticate using the existing profile.

Error Message `You chose not to copy your private PAC. If you experience wireless connection problems during Windows domain logon or logged off stage, you must reconfigure the profile to use a global PAC.`

Explanation When you were prompted to copy your PAC to the global store so that it will be available when you are not logged on, you clicked No.

Recommended Action The profile will use the private PAC for authentication. However, if you experience any wireless connection problems, you may need to reconfigure your profile to use a global PAC.

Error Message `You do not have a valid Protected Access Credentials (PAC), the PAC you provided does not match the authentication server, or the PAC is expired. You may proceed with authenticating if the server supports auto provisioning. Do you want to proceed and accept auto provisioning?`

Explanation You activated an EAP-FAST profile that is configured for automatic PAC provisioning and does not specify a PAC authority for which you have a current valid PAC.

Recommended Action If you want to attempt to auto-provision a PAC from the server, click **Yes**. Otherwise, click **No**. If you choose No, a message appears indicating that the client adapter was unable to EAP-FAST authenticate.

Error Message `You failed to change your EAP-FAST domain/network password. Make sure you enter a new password that complies with the password policy and try again. Do you want to retry now?`

Explanation An error occurred when you attempted to change your EAP-FAST password.

Recommended Action Click **Yes** to try again. When the Enter Wireless Network Password window appears, enter your new password. Otherwise, click **No** to cancel the operation.

Error Message `You have just changed your network password. You must change your saved password settings in the EAP-FAST profiles before connecting again.`

Explanation Your network password has changed.

Recommended Action Update your EAP-FAST password on the EAP-FAST Settings window for any EAP-FAST profiles that are configured with a saved username and password.

Error Message `You must configure the PEAP-GTC settings properly. User information, password, or machine information is incomplete.`

Explanation You improperly configured a PEAP (EAP-GTC) profile.

Recommended Action Modify the profile's configuration settings, making sure to enter all necessary information.

Error Message `You must enter the correct old password in order to change the new password.`

Explanation You incorrectly entered your old EAP-FAST password on the Please Change Password window.

Recommended Action Carefully re-enter your old EAP-FAST password on the Please Change Password window.

Error Message `You must select a PAC or enable Allow Automatic PAC Provisioning.`

Explanation While configuring a profile for EAP-FAST, you did not enable automatic PAC provisioning or select a PAC authority from the drop-down list on the EAP-FAST Settings window.

Recommended Action Choose a PAC authority from the drop-down list on the EAP-FAST Settings window. If the list is empty, import a PAC file.

Error Message `You must select a Passphrase to use Pre-Shared keys and WPA/WPA2.`

Explanation You chose the WPA/WPA2 Passphrase option on the Profile Management (Security) window and clicked **OK** without entering a Passphrase.

Recommended Action Enter a WPA/WPA2 Passphrase on the Define WPA/WPA2 Pre-Shared Key window.

Error Message `You must set at least one Pre-Shared Key.`

Explanation You chose the Pre-Shared Key (Static WEP) option on the Profile Management (Security) window and clicked **OK** without entering a static WEP key.

Recommended Action Enter a static WEP key on the Define Pre-Shared Keys window and then click **OK**.

Error Message `Your security setting is invalid for an Ad Hoc network. If you want, security will be disabled for you. You can also configure security to Pre-shared keys. Do you want to disable security?`

Explanation Pre-Shared Key (Static WEP) is the only valid security option for an ad hoc network. You chose Ad Hoc for Network Type on the Profile Management (Advanced) window when a security option other than static WEP was already selected.

Recommended Action If you want to configure this profile for use in an ad hoc network, click **Yes** to disable security. Otherwise, click **No**.

Error Message `You selected a private PAC for EAP-FAST authentication. It may not be accessible when the user is logged off or during the domain logon process. Confirm if you want to copy the selected PAC into the global PAC store.`

Explanation You selected a private PAC and the No Network Connection Unless User Is Logged In check box is unchecked. Therefore, the PAC may not be accessible during domain logon or when you are logged off.

Recommended Action If you want a copy of the PAC to be added to the global store so that it will be available when you are not logged on, click **Yes**. If you do not want a copy of the PAC to be added to the global store, click **No**.

Technical Specifications

This appendix provides technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Physical Specifications, page A-2
- Radio Specifications, page A-2
- Power Specifications, page A-6
- Safety and Regulatory Compliance Specifications, page A-6

Table A-1 lists the technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters

Physical Specifications	
Size	
PC-Cardbus card	4.5 in. L x 2.1 in. W x 0.2 in. H (11.3 cm L x 5.4 cm W x 0.5 cm H)
PCI card	
Standard PCI card	4.7 in. L x 0.7 in. W x 4.8 in. H (12 cm L x 1.8 cm W x 12.1 cm H)
Low-profile PCI card	4.7 in. L x 0.7 in. W x 3.1 in. H (12 cm L x 1.8 cm W x 7.9 cm H)
Weight	
PC-Cardbus card	1.55 oz (44 g)
PCI card	
Standard PCI card with antenna	3.6 oz (103 g)
Standard PCI card without antenna	1.9 oz (55 g)
Low-profile PCI card with antenna	3.5 oz (98 g)
Low-profile PCI card without antenna	1.7 oz (49 g)
Enclosure	
PC-Cardbus card	Type II Cardbus
PCI card	Standard or low-profile Type II PCI
Connector	
PC-Cardbus card	68-pin Cardbus
PCI card	62-pin PCI
Status indicators	Green and amber LEDs; see Chapter 10
Operating temperature	32°F to 158°F (0°C to 70°C)
Storage temperature	32°F to 185°F (0°C to 85°C)
Humidity (non-operational)	90% relative humidity
ESD	15 kV (human body model)
Radio Specifications	
Type	
802.11a	Orthogonal frequency division multiplexing (OFDM)
802.11b/g	Direct-sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM)

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Power output **Note** Refer to Appendix D for limitations on radiated power (EIRP) levels in the European community and other countries.	
802.11a	40 mW (16 dBm) @ 6, 9, 12, 18, 24 Mbps 25 mW (14 dBm) @ 6, 9, 12, 18, 24, 36 Mbps 20 mW (13 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps 13 mW (11 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps 10 mW (10 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps **Note** The maximum power setting varies according to individual country regulations.
802.11b/g	100 mW (20 dBm) @ 1, 2, 5.5, 11 Mbps 63 mW (18 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24 Mbps 50 mW (17 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 Mbps 30 mW (15 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 Mbps 20 mW (13 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps 10 mW (10 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps **Note** The maximum power setting varies according to individual country regulations.
Operating frequency	
802.11a	5.15 to 5.25 GHz in the UNII 1 band* 5.25 to 5.35 GHz in the UNII 2 band* 5.470 to 5.725 GHz in the European band 5.725 to 5.825 GHz in the UNII 3 band* *Depending on the regulatory domain in which the client adapter is used
802.11b/g	2.400 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)
Usable channels	
802.11a	5150 to 5350 MHz and 5725 to 5825 MHz
802.11b/g	2412 to 2484 MHz in 5-MHz increments
Data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Modulation	Differential binary phase shift keying (DBPSK) - 1 Mbps Differential quaternary phase shift keying (DQPSK) - 2 Mbps Complementary code keying (CCK) - 5.5 and 11 Mbps Binary phase shift keying (BPSK) - 6 and 9 Mbps Quaternary phase shift keying (QPSK) - 12 and 18 Mbps 16-quadrate amplitude modulation (16-QAM) - 24 and 36 Mbps 64-quadrate amplitude modulation (64-QAM) - 48 and 54 Mbps

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Receiver sensitivity	
802.11a	**5150 to 5250 MHz** –87 dBm @ 6, 9, 12, and 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –74 dBm @ 48 Mbps –72 dBm @ 54 Mbps **5250 to 5350 MHz** –89 dBm @ 6, 9, and 12 Mbps –85 dBm @ 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –74 dBm @ 48 Mbps –72 dBm @ 54 Mbps **5470 to 5725 MHz** –87 dBm @ 6, 9, 12, and 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –74 dBm @ 48 Mbps –72 dBm @ 54 Mbps **5725 to 5805 MHz** –84 dBm @ 6, 9, and 12 Mbps –83 dBm @ 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –72 dBm @ 48 Mbps –65 dBm @ 54 Mbps
802.11b/g	–94 dBm @ 1 Mbps –93 dBm @ 2 Mbps –92 dBm @ 5.5 Mbps –90 dBm @ 11 Mbps –86 dBm @ 6, 9, 12, and 18 Mbps –84 dBm @ 24 Mbps –80 dBm @ 36 Mbps –75 dBm @ 48 Mbps –71 dBm @ 54 Mbps

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Receiver delay spread (multipath)		
802.11a/g	400 ns @ 6 Mbps 250 ns @ 9 and 12 Mbps 220 ns @ 18 Mbps 160 ns @ 24 Mbps 100 ns @ 36 Mbps 90 ns @ 48 Mbps 70 ns @ 54 Mbps	
802.11b	350 ns @ 1 Mbps 300 ns @ 2 Mbps 200 ns @ 5.5 Mbps 130 ns @ 11 Mbps	
Range		
802.11a	**Indoor (typical)** 500 ft (152 m) @ 6 Mbps 400 ft (122 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps	**Outdoor (typical)** 950 ft (290 m) @ 6 Mbps 800 ft (244 m) @ 18 Mbps 170 ft (52 m) @ 54 Mbps
	Note The above range numbers assume that the client adapter is being used at maximum transmit power with a Cisco Aironet 1232AG Access Point with a 3.5-dBi dipole antenna. Different range characteristics are likely when using the client adapter with a different access point or a Cisco Aironet 1200 Series Access Point with a different antenna.	
802.11b/g	**Indoor (typical)** 410 ft (125 m) @ 1 Mbps 300 ft (91 m) @ 6 Mbps 220 ft (67 m) @ 11 Mbps 180 ft (55 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps	**Outdoor (typical)** 700 ft (213 m) @ 1 Mbps 650 ft (198 m) @ 6 Mbps 490 ft (149 m) @ 11 Mbps 400 ft (122 m) @ 18 Mbps 110 ft (34 m) @ 54 Mbps
	Note The above range numbers assume that the client adapter is being used at maximum transmit power with a Cisco Aironet 1232AG Access Point with a 2.2-dBi dipole antenna. Different range characteristics are likely when using the client adapter with a different access point or a Cisco Aironet 1200 Series Access Point with a different antenna.	

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Antennas	
PC-Cardbus card	Integrated 0-dBi dual-band 2.4/5-GHz diversity antenna
PCI card	1-dBi dual-band 2.4/5-GHz antenna, permanently attached by 6.6-ft (2-m) cable
Power Specifications	
Operational voltage	3.3 V (± 0.3 V)
Receive current steady state	
802.11a	318 mA maximum
802.11b	327 mA maximum
802.11g	282 mA maximum
Transmit current steady state	
802.11a	554 mA maximum
802.11b	539 mA maximum
802.11g	530 mA maximum
Sleep mode steady state	203 mA average
Safety and Regulatory Compliance Specifications	
Safety	Designed to meet: • UL 60950 • CSA 22.2 No. 60950 • IEC 60950 Second Ed., including Amendments 1-4 with all national deviations • EN 60950 Second Ed., including Amendments 1-4
EMI and susceptibility	FCC Part 15.107 & 15.109 Class B ICES-003 Class B (Canada) VCCI (Japan) EN 301.489-1 and EN-301.489-17 (Europe)
Radio approvals	FCC Part 15.247 FCC Part 15.401-15.407 Canada RSS-210 Europe EN-300.328, EN-301.893 ARIB STD-33, ARIB STD-66, ARIB STD-T71 (Japan) AS 4268.2 (Australia) AS/NZS 3548 (Australia and New Zealand)
RF exposure	FCC Bulletin OET-65C Industry Canada RSS-102

Translated Safety Warnings

This appendix provides translations of the safety warnings that appear in this publication. The second warning pertains to the PI21AG client adapter, and the third warning pertains to the CB21AG client adapter.

The following topics are covered in this appendix:

- Explosive Device Proximity Warning, page B-2
- Antenna Installation Warning, page B-3
- Warning for Laptop Users, page B-4

Explosive Device Proximity Warning

Warning	**Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**
Waarschuwing	**Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermde ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.**
Varoitus	**Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.oen.**
Attention	**Ne jamais utiliser un équipement de réseau sans fil à proximité d'un détonateur non blindé ou dans un lieu présentant des risques d'explosion, sauf si l'équipement a été modifié à cet effet.**
Warnung	**Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.**
Avvertenza	**Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.**
Advarsel	**Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.**
Aviso	**Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.**
¡Advertencia!	**No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.**
Varning!	**Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.**

Antenna Installation Warning

Warning	In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.
Waarschuwing	Om te voldoen aan de FCC radiofrequentie (RF) blootstellingslimieten dienen antennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.
Varoitus	FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan antennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.
Attention	Pour se conformer aux limites d'exposition à la fréquence radio préconisées par la FCC (Federal Communications Commission), les antennes doivent se situer à un minimum de 20 cm de toute personne.
Warnung	Um die in den FCC-Richtlinien festgelegten Expositionshöchstgrenzen für Radiofrequenzen (RF) nicht zu überschreiten, sollten antennen mindestens 20 cm (7,9 Zoll) vom Körper aller Person entfernt aufgestellt werden.
Avvertenza	Per conformarsi ai limiti FCC di esposizione a radiofrequenza (RF), le antenne a devono stare ad una distanza minima di 20 cm dal corpo di ogni persona.
Advarsel	I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal antenner befinne seg på en avstand av minst 20 cm eller mer fra mennesker.
Aviso	Para estar de acordo com as normas FCC de limites de exposição para freqüência de rádio (RF), as antenas devem estar distantes no mínimo 20 cm (7,9 pol) do corpo de qualquer pessoa.
¡Advertencia!	Para cumplir con los límites de exposición de radio frecuencia (RF) de la Comisión Federal de Comunicaciones (FCC) es preciso ubicar las antenas a un mínimo de 20 cm (7,9 pulgadas) o más del cuerpo de las personas.
Varning!	För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör antenner placeras på minst 20 cm avstånd från alla människor.

Warning for Laptop Users

Warning **This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PC Card slots that can provide at least 0.394 in (1 cm) separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.**

Waarschuwing **Dit apparaat is getest en voldoet aan de FCC-beperkingen voor radiofrequentieblootstelling (SAR) bij standaardconfiguraties met een laptopcomputer. Dit apparaat kan worden gebruikt in desktop- of laptopcomputers met PC-kaartsleuven aan de zijkant, waarbij minimaal 1 cm afstand bestaat tussen de antenne en het lichaam van de gebruiker of een persoon in de buurt. Bij smalle laptopcomputers is mogelijk extra aandacht vereist om tijdens gebruik voldoende afstand tot de antenne te houden. Dit apparaat kan niet worden gebruikt in combinatie met mobiele PDA's (personal digital assistants; persoonlijke digitale assistenten). Als u dit apparaat gebruikt in andere configuraties, voldoet het wellicht niet meer aan de FCC-regelgeving met betrekking tot radiofrequentieblootstelling. Dit apparaat en de bijbehorende antenne mogen niet in combinatie met andere antennes of zenders worden gebruikt en ook niet in de buurt van andere antennes of zenders worden geplaatst.**

Varoitus **Tämä laite on testattu ja se noudattaa FCC:n määrittämiä radiotaajuussäteilylle altistumisen (SAR) raja-arvoja tyypillisissä kannettavien tietokoneiden kokoonpanoissa. Tätä laitetta voidaan käyttää pöytä- tai kannettavissa tietokoneissa, joiden sivussa on PC-korttipaikka. Korttipaikassa olevan laitteen antennin etäisyyden käyttäjästä tai lähellä olevasta henkilöstä on oltava vähintään yksi senttimetri. Ohuita kannettavia tietokoneita on ehkä tarkkailtava erityisesti, jotta käyttäjän etäisyys antenniin olisi riittävä käytön aikana. Tätä laitetta ei voi käyttää yhdessä kämmentietokoneiden (PDA) kanssa. Jos laitetta käytetään muunlaisissa kokoonpanoissa, se ei ehkä vastaa FCC:n määrittämiä radiotaajuussäteilylle altistumisen ohjearvoja. Tätä laitetta ja sen antennia ei saa käyttää samassa pisteessä toisen antennin tai lähettimen kanssa tai liitettynä toiseen antenniin tai lähettimeen.**

Attention **Cet appareil a été testé et respecte les limites (TAS - Taux d'absorption spécifique) d'exposition aux RF de la FCC relatives aux configurations standard des ordinateurs portables. Il peut être utilisé dans des ordinateurs de bureau ou portables dotés d'un emplacement pour carte PC latérales et peut fournir une distance de séparation d'au moins 1 cm entre l'antenne et le corps de l'utilisateur ou d'une personne avoisinante. Nous vous recommandons de porter une attention particulière lors de l'utilisation d'ordinateurs portatifs minces afin d'assurer le maintien de l'espacement de l'antenne. Cet appareil ne peut pas être utilisé avec des assistants numériques personnels de poche. L'utilisation dans d'autres configurations risque de ne pas être conforme aux lignes directrices de la FCC sur l'exposition aux RF. Cet appareil et son antenne ne doivent pas se trouver dans le même emplacement ou fonctionner conjointement avec une autre antenne ou un autre émetteur.**

Warnung **Dieses Gerät wurde getestet und entspricht den durch die FCC-Richtlinien festgelegten Grenzwerten für Hochfrequenzstrahlung (SAR) für reguläre Laptop-Computerkonfigurationen. Es kann für Desktop- oder Laptop-Computer mit seitlichem PC-Kartensteckplatz genutzt werden, wobei der Abstand der Antenne vom Benutzer oder anderen in der Nähe befindlichen Personen mindestens 1 cm betragen muss. Insbesondere bei schmalen Laptop-Computern sollte darauf geachtet werden, dass der Abstand während des Betriebs genau eingehalten wird. Dieses Gerät kann nicht für tragbare Handheld-Geräte/PDAs verwendet werden. Bei Verwendung in anderen Konfigurationen ist u.U. die Einhaltung der durch die FCC-Richtlinien festgelegten Grenzwerte für Hochfrequenzstrahlung nicht gewährleistet. Dieses Gerät und die Antenne dürfen nicht zusammen mit anderen Antennen oder Übertragungsgeräten installiert oder verwendet werden.**

Avvertenza **Questo dispositivo è stato testato ed è conforme alle norme sulle emissioni radio (SAR) nelle configurazione tipica di computer portatile. Questo dispositivo può essere utilizzato in desktop o computer portatili con slot per scheda PC laterale che garantisca un minimo spazio di 1 cm (0,394 pollici) tra l'antenna e l'utente o qualsiasi persona nelle vicinanze. I computer portatili sottili richiedono particolare attenzione al mantenimento dello spazio minimo quando in funzione. Questo dispositivo non può essere utilizzaato con computer palmari (PDA). L'utilizzo in configurazione differenti non assicura la conformità alle norme sulle emissioni radio. Questo dispositivo e la propria antenna non devono operare congiuntamente and altre antenne o trasmettitori.**

Advarsel **Denne enheten er testet og overholder grensene for FCC RF-eksponering (SAR) i vanlige konfigurasjoner for bærbare datamaskiner. Den kan brukes i stasjonære eller bærbare datamaskiner som har kortplass på siden, og der det er minst 1 cm avstand mellom antennen og brukeren eller andre personer. Ved bruk av flate bærbare PCer må du være ekstra påpasselig med antenneavstanden. Denne enheten kan ikke brukes sammen med håndholdte PDAer (personal digital assistant). Det er ikke sikkert at bruk i andre konfigurasjoner vil være i samsvar med retningslinjene for FCC RF-eksponering. Denne enheten og antennen må ikke plasseres på samme sted som eller brukes sammen med andre antenner eller sendere.**

Aviso **Este dispositivo foi testado e está em conformidade com os limites SAR de exposição a radiofrequência (RF) da Comissão Federal de Comunicações (FCC), em configurações típicas de portátil, e pode ser utilizado em computadores de secretária ou portáteis com ranhuras de placa PC laterais que permitem um distanciamento mínimo de 1cm. entre a antena e o corpo do utilizador ou de alguém que esteja por perto. Os portáteis finos necessitam de uma atenção especial para manter a distância da antena durante o funcionamento. Este dispositivo não pode ser utilizado com PDAs (personal digital assistants) de mão. A utilização noutras configurações pode não assegurar a conformidade com as directrizes de exposição a radiofrequência (RF) da Comissão Federal de Comunicações (FCC). Este dispositivo e a respectiva antena não devem ser colocados nem postos a funcionar com outras antenas ou transmissores.**

¡Advertencia! **El dispositivo ha sido probado y cumple los límites de la FCC sobre exposición a radiofrecuencia (SAR o tasa de absorción específica) en cualquier configuración tradicional de equipos portátiles. Además, puede utilizarse en equipos de escritorio o portátiles que cuenten con ranuras de tarjeta PC laterales a una distancia de, al menos, 1 cm (0,394 pulgadas) de la antena al usuario o persona más cercana. Puede que los equipos portátiles de menor grosor requieran atención especial a la hora de mantener la distancia de la antena al utilizarlos. No puede utilizarse este dispositivo con equipos digitales personales portátiles (PDA). Su utilización en otras configuraciones no garantiza el cumplimiento de las directivas de la FCC sobre exposición a radiofrecuencia. Este dispositivo y la antena no deben situarse o accionarse junto con otra antena o transmisor.**

Varning! **Den här enheten har testats och följer FCC-gränserna för radiofrekvensexponering (SAR) i vanliga konfigurationer för bärbara datorer. Den kan användas i stationära eller bärbara datorer med sidmonterade PC-kortöppningar som kan tillhandahålla minst 1 cm med separationsavstånd mellan antennen och användarens kropp eller annan person i närheten. Tunna, bärbara datorer kan behöva speciell uppmärksamhet för att upprätthålla antennavståndet under användning. Den här enheten kan inte användas med handdator/PDA. Vid användning i andra konfigurationer går det inte att garantera att FCC:s riktlinjer för radiofrekvens följs. Den här enheten och dess antenn får inte placeras tillsammans med eller användas i samband med någon annan antenn eller sändare/mottagare.**

Figyelem **Az eszköz tesztelésen esett át, melynek eredményeként megfelel az FCC RF-sugárzási (SAR) korlátozásainak tipikus laptop-konfigurációk esetén. Az eszköz beszerelhető asztali és laptop számítógépekben lévő, oldalra szerelt PC-kártya csatlakozókba, amennyiben legalább 1 cm távolság van az antenna és a felhasználó vagy egy közeli személy teste között. Vékony laptop számítógépek esetén különösen ügyelni kell használat közben az antennától való távolság betartására. Az eszköz nem használható kézi PDA-kkal (személyi digitális asszisztensekkel). Más konfigurációk esetén előfordulhat, hogy az eszköz nem felel meg az FCC RF-sugárzási előírásainak. Az eszközt és annak antennáját nem szabad más antennával vagy adó-vevővel egy helyen elhelyezni vagy üzemeltetni.**

Предупреждение **Это устройство протестировано и признано соответствующим ограничениям FCC, касающимся высокочастотного излучения (SAR), для обычных конфигураций портативных компьютеров. Оно может использоваться на переносных или портативных компьютерах с боковыми гнездами для плат PC, которые обеспечивают зазор не менее 0,394 дюйма (1 см) между антенной и телом пользователя или другого лица, находящегося в непосредственной близости. Возможно, потребуется соблюдать особую осторожность при обеспечении зазора антенны в тонких портативных компьютерах. Это устройство нельзя использовать для карманных компьютеров. Использование в других конфигурациях не может гарантировать соответствие директивам FCC, касающимся высокочастотного излучения. Это устройство и его антенну нельзя располагать рядом или использовать совместно с другой антенной или передатчиком.**

警告 将本设备用于典型膝上型计算机配置已经过测试并且符合 FCC RF 辐射暴露（SAR）限制；本设备可用于侧面安装有 PC 卡插槽的台式计算机或膝上型计算机，该插槽可确保用户或周围的人与天线至少相距 0.394 英寸（1 厘米）。使用超薄膝上型计算机时，可能需要特别注意在操作过程中与天线保持一定距离。本设备不能与手持式 PDA（个人数字助理）一起使用。在其他配置中使用本设备可能无法确保符合 FCC RF 辐射暴露限制规定。禁止将本设备及其天线与任何其他天线或发射器安装在一起或同时使用。

警告 この機器は既にテスト済みで、一般的なラップトップ コンピュータの構成における米国 FCC（連邦通信委員会）の無線周波（RF）照射（SAR）制限値に準拠しています。この機器は、デスクトップ コンピュータもしくは本体側面に PC カード スロットを備えたラップトップ コンピュータでの使用が可能です。いずれのコンピュータの場合も、アンテナと人体との間に、最低 1 cm の距離があることが前提です。薄型のラップトップ コンピュータの場合は、操作中アンテナとのスペースを維持するため、特別な注意が必要になることがあります。この機器は、ハンドヘルド式の PDA（携帯情報端末）には使用できません。他の配置構成での使用は、FCC の無線周波照射に関するガイドラインに準拠しない場合があります。この機器およびアンテナは、他のアンテナもしくはトランスミッタと同一の場所に配置したり、同時に使用してはなりません。

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Manufacturer's Federal Communication Commission Declaration of Conformity Statement, page C-2
- Department of Communications – Canada, page C-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein, page C-3
- Declaration of Conformity for RF Exposure, page C-7
- Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan, page C-7
- Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan, page C-8

Manufacturer's Federal Communication Commission Declaration of Conformity Statement

Models: AIR-CB21AG-A-K9, AIR-PI21AG-A-K9

FCC Certification Number: LDK102050 (CB21AG)
LDK102051 (PI21AG)

Manufacturer: Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The CB21AG client adapter has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations, and this device can be used in laptop computers with side-mounted PCMCIA slots which can provide 0.394 in (1 cm) separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating.

The PI21AG client adapter has been tested and complies with FCC RF Exposure (SAR) limits in typical desktop computer configurations. A separation distance of 7.9 in (20 cm) must be maintained between this device's antenna and the body of the user or a nearby person.

These devices cannot be used with handheld personal digital assistants (PDAs). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. These devices and their antennas must not be co-located or operated in conjunction with any other antenna or transmitter.

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

Caution Within the 5.15-to-5.25-GHz band, UNII devices are restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite Systems (MSS) operations.

Department of Communications – Canada

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters are certified to the requirements of RSS-210 for 2.4-GHz and 5-GHz devices. The use of these devices in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprecheneden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Directiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directive 1999/5/EC.
Έλληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigencies essentialles et aux autres dispositions pertinantes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.

Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-directiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

The Declaration of Conformity related to this product can be found at the following URL:

http://www.ciscofax.com

The following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2 (2.4-GHz operation);
  EN 301.893 (5-GHz operation)
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

The following CE mark is affixed to the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters:

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact your customer service representative.

Declaration of Conformity Statement

Cisco Aironet CB21AG Wireless LAN Client Adapter

CISCO SYSTEMS

DECLARATION OF CONFORMITY
with regard to the R&TTE Directive 1999/5/EC
according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134 - USA

Declare under our sole responsibility that the product,

AIR-CB21AG-E-K9 / Cisco Aironet 802.11a/b/g Wireless CardBus Adapter

Fulfils the essential requirements of the Directive 1999/5/EC.

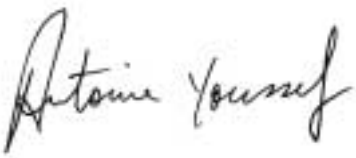
The following standards were applied:

EMC	**EN 301.489-1** v1.4.1**: 2002-08; EN 301.489-17** v1.2.1**: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328** v1.4.1**: 2003-04** **EN 301.893** v1.2.3**: 2003-08**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark: CE !

Date & Place of Issue: 1 January 2004, San Jose

Signature: 

Tony Youssef
Director Corporate Compliance
125 West Tasman Drive
San Jose, CA 95134 - USA

DofC 340347

Cisco Aironet PI21AG Wireless LAN Client Adapter

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134 - USA

Declare under our sole responsibility that the product,

AIR-PI21AG-E-K9 / Cisco Aironet 802.11a/b/g Wireless PCI Adapter

Fulfils the essential requirements of the Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301.489-1** v1.4.1**: 2002-08; EN 301.489-17** v1.2.1**: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328** v1.4.1**: 2003-04** **EN 301.893** v1.2.3**: 2003-08**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark: CE 0

Date & Place of Issue: 1 January 2004, San Jose

Signature:

Tony Youssef
Director Corporate Compliance
125 West Tasman Drive
San Jose, CA 95134 - USA

DofC 340350

Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet Wireless LAN Client Adapters in Japan. These guidelines are provided in both Japanese and English.

Note The use of 5-GHz devices is limited to indoor use in Japan.

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。

2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。

3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-5549-6500

43768

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-5549-6500

Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan

This section provides administrative rules for operating Cisco Aironet Wireless LAN Client Adapters in Taiwan. The rules are provided in both Chinese and English.

2.4- and 5-GHz Client Adapters

Chinese Translation

低功率電波輻射性電機管理辦法

第十四條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

117710

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 17

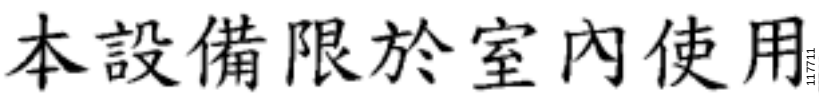
The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with COMMUNICATION ACT.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

5-GHz Client Adapters

Chinese Translation



English Translation

This equipment is limited for indoor use.

Channels, Power Levels, and Antenna Gains

This appendix lists the IEEE 802.11a, b, and g channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per data rate.

The following topics are covered in this appendix:

- Channels, page D-2
- Maximum Power Levels and Antenna Gains, page D-4

Channels

IEEE 802.11a

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are shown in Table D-1.

Table D-1 Channels for IEEE 802.11a

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		America (-A)	EMEA (-E)	Japan (-J)	Rest of World (-W)
34	5170	–	–	X	–
36	5180	X	X	–	X
38	5190	–	–	X	–
40	5200	X	X	–	X
42	5210	–	–	X	–
44	5220	X	X	–	X
46	5230	–	–	X	–
48	5240	X	X	–	X
52	5260	X	X	–	X
56	5280	X	X	–	X
60	5300	X	X	–	X
64	5320	X	X	–	X
100	5500	–	X	–	X
104	5520	–	X	–	X
108	5540	–	X	–	X
112	5560	–	X	–	X
116	5580	–	X	–	X
120	5600	–	X	–	X
124	5620	–	X	–	X
128	5640	–	X	–	X
132	5660	–	X	–	X
136	5680	–	X	–	X
140	5700	–	X	–	X
149	5745	X	–	–	X
153	5765	X	–	–	X
157	5785	X	–	–	X
161	5805	X	–	–	X

Note All channel sets are restricted to indoor usage except America (-A), which allows for indoor and outdoor use on channels 52 through 161 in the United States.

IEEE 802.11b/g

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b/g 22-MHz-wide channel are shown in Table D-2.

Table D-2 Channels for IEEE 802.11b/g

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		America (-A)	EMEA (-E)	Japan (-J)	Rest of World (-W)
1	2412	X	X	X	X
2	2417	X	X	X	X
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467	–	X	X	X
13	2472	–	X	X	X
14	2484	–	–	X	–

Note Mexico is included in the Rest of World regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.

Note In Japan, channel 14 is not supported for 802.11g mode.

Maximum Power Levels and Antenna Gains

IEEE 802.11a

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table D-3 indicates the maximum EIRP allowed for each data rate in the IEEE 802.11a regulatory domains.

Table D-3 Maximum EIRP for IEEE 802.11a

	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
Data Rate	**mW**	**dBm**
6 Mbps	40	16
9 Mbps	40	16
12 Mbps	40	16
18 Mbps	40	16
24 Mbps	40	16
36 Mbps	25.1	14
48 Mbps	20	13
54 Mbps	20	13

IEEE 802.11b

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table D-4 indicates the maximum EIRP allowed for each data rate in the IEEE 802.11b regulatory domains.

Table D-4 Maximum EIRP for IEEE 802.11b

	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
Data Rate	**mW**	**dBm**
1 Mbps	100	20
2 Mbps	100	20
5.5 Mbps	100	20
11 Mbps	100	20

IEEE 802.11g

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table D-5 indicates the maximum EIRP allowed for each data rate in the IEEE 802.11g regulatory domains.

Table D-5 Maximum EIRP for IEEE 802.11g

	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
Data Rate	**mW**	**dBm**
6 Mbps	50	17
9 Mbps	50	17
12 Mbps	50	17
18 Mbps	50	17
24 Mbps	50	17
36 Mbps	40	16
48 Mbps	31.6	15
54 Mbps	20	13

Configuring the Client Adapter through the Windows XP Operating System

This appendix explains how to configure and use the client adapter with Windows XP.

The following topics are covered in this appendix:

- Overview, page E-2
- Configuring the Client Adapter, page E-5
- Associating to an Access Point Using Windows XP, page E-18
- Viewing the Current Status of Your Client Adapter, page E-18

Overview

This appendix provides instructions for minimally configuring the client adapter through the Microsoft Wireless Configuration Manager in Windows XP (instead of through ADU) as well as for enabling the security options that are available for use with this operating system. The "Overview of Security Features" section below describes each of these options so that you can make an informed decision before you begin the configuration process.

In addition, this appendix also provides basic information on using Windows XP to specify the networks to which the client adapter associates and to view the current status of your client adapter.

Note If you require more information about configuring or using your client adapter with Windows XP, refer to Microsoft's documentation for Windows XP.

Overview of Security Features

When you use your client adapter with Windows XP, you can protect your data as it is transmitted through your wireless network by encrypting it through the use of wired equivalent privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the EAP authentication process. The information in the "Static WEP Keys" and "EAP (with Dynamic WEP Keys)" sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

WEP keys, whether static or dynamic, are either 40 or 128 bits in length. 128-bit WEP keys offer a greater level of security than 40-bit WEP keys.

Static WEP Keys

Each device within your wireless network can be assigned up to four static WEP keys. If a device receives a packet that is not encrypted with the appropriate key (as the WEP keys of all devices that are to communicate with each other must match), the device discards the packet and never delivers it to the intended receiver.

You do not need to re-enter static WEP keys each time the client adapter is inserted or the Windows device is rebooted because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter's registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

EAP (with Dynamic WEP Keys)

The standard for wireless LAN security, as defined by IEEE, is called *802.1X for 802.11*, or simply *802.1X*. An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network.

Two 802.1X authentication types are available when configuring your client adapter through Windows XP:

- **EAP-TLS**—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.

  RADIUS servers that support EAP-TLS include Cisco Secure ACS release 3.0 or later and Cisco Access Registrar release 1.8 or later.

- **Protected EAP** (or **PEAP**)—One of the following PEAP authentication types are available, depending on the software that is installed on your computer:

  – **PEAP (EAP-MSCHAP V2)**—This PEAP authentication type is available if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was not previously installed on your computer or was installed prior to Service Pack 1 for Windows XP.

    PEAP (EAP-MSCHAP V2) authentication is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

    RADIUS servers that support PEAP (EAP-MSCHAP V2) authentication include Cisco Secure ACS release 3.2 or later.

  – **PEAP (EAP-GTC)**—Although this authentication type is not officially supported for CB21AG and PI21AG client adapters, you may be able to use it successfully if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was previously installed on your computer and installed after Service Pack 1 for Windows XP.

    PEAP (EAP-GTC) authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. PEAP (EAP-GTC) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. If your network uses an OTP user database, PEAP (EAP-GTC) requires you to enter either a hardware token password or a software token PIN to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (EAP-GTC) requires you to enter your username, password, and domain name in order to start the authentication process.

    RADIUS servers that support PEAP (EAP-GTC) authentication include Cisco Secure ACS release 3.1 or later and Cisco Access Registrar release 3.5 or later.

When you enable EAP on your access point and configure your client adapter for EAP-TLS or PEAP using Windows XP, authentication to the network occurs in the following sequence:

1. The client adapter associates to an access point and begins the authentication process.

Note The client does not gain full access to the network until authentication between the client and the RADIUS server is successful.

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (PEAP) or certificate (EAP-TLS) being the shared secret for authentication. The password is never transmitted during the process.
3. If authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.
4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.
5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets (and broadcast packets if the access point is set up to do so) that travel between them.

Note Refer to the IEEE 802.11 Standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ab.html

WPA

Wi-Fi Protected Access (WPA) is a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection and 802.1X for authenticated key management.

WPA supports two mutually exclusive key management types: WPA and WPA passphrase (also known as *WPA pre-shared key* or *WPA-PSK*). Using WPA, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). The server generates the PMK dynamically and passes it to the access point. Using WPA passphrase, however, you configure a passphrase (or pre-shared key) on both the client and the access point, and that passphrase is used as the PMK.

In order to use WPA, your computer must be running Windows XP Service Pack 2.

Note WPA must also be enabled on the access point. Access points must use Cisco IOS Release 12.2(11)JA or later to enable WPA. Refer to the documentation for your access point for instructions on enabling this feature.

Configuring the Client Adapter

Follow the steps below to configure your client adapter using Windows XP.

Note These instructions assume you are using the Windows XP classic view rather than the category view. Otherwise, the windows you see will look different than those shown in this section.

Note The appropriate certificates must be installed on your computer if you are planning to enable EAP-TLS or PEAP authentication. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate. Contact your system administrator if you need help obtaining and importing the necessary certificates.

Step 1 Make sure the client adapter's driver has been installed and the client adapter is inserted in the Windows XP device.

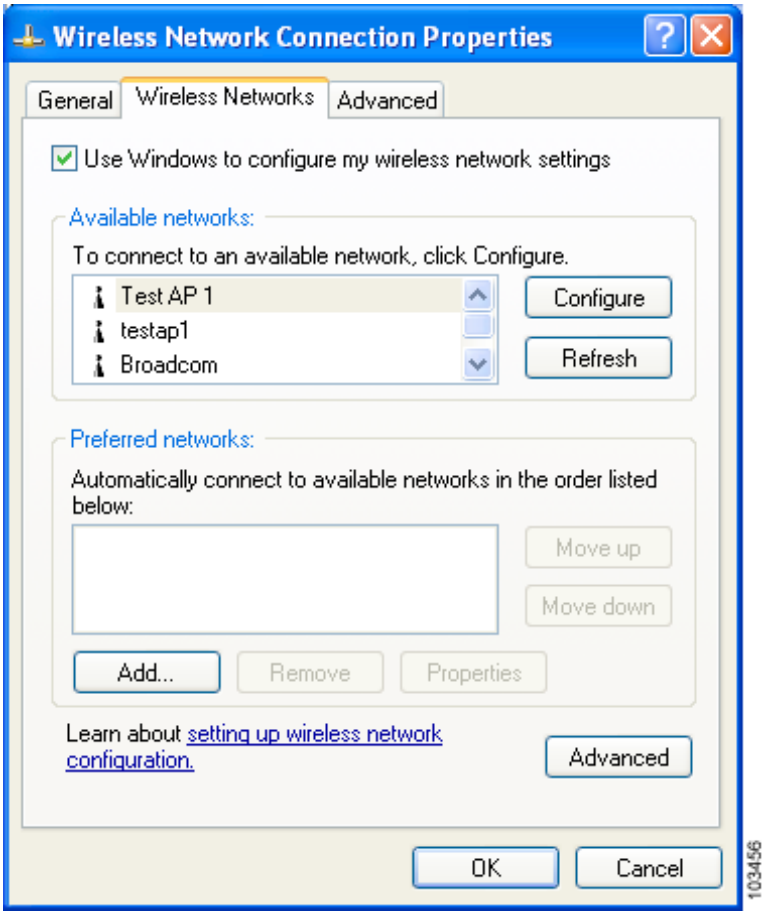
Step 2 Double-click **My Computer**, **Control Panel**, and **Network Connections**.

Step 3 Right-click **Wireless Network Connection**.

Step 4 Click **Properties**. The Wireless Network Connection Properties window appears.

Step 5 Click the **Wireless Networks** tab. The following window appears (see Figure E-1).

Figure E-1 Wireless Network Connection Properties Window (Wireless Networks Tab)



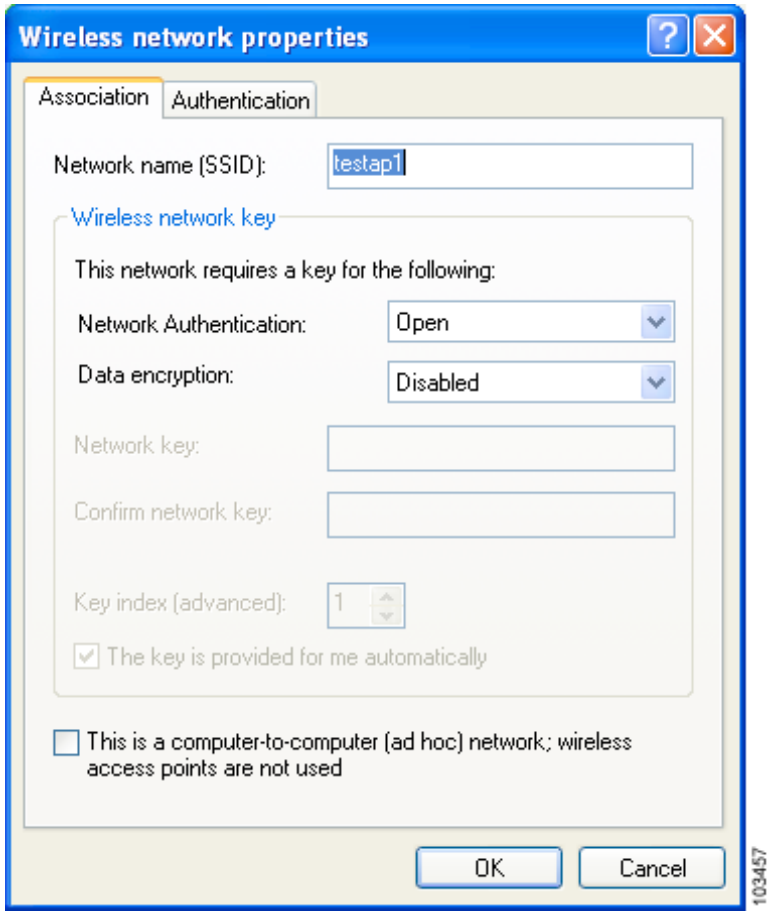
Step 6 Make sure that the **Use Windows to configure my wireless network settings** check box is checked.

Step 7 Choose the SSID of the access point to which you want the client adapter to associate from the list of available networks and click **Configure**. If the SSID of the access point you want to use is not listed or you are planning to operate the client adapter in an *ad hoc network* (a computer-to-computer network without access points), click **Add**.

Note The Allow Broadcast SSID to Associate option on the access point must be enabled for the SSID to appear in the list of available networks.

The Wireless Network Properties window appears (see Figure E-2).

Figure E-2 Wireless Network Properties Window (Association Tab)



Step 8 Perform one of the following:

- If you chose an SSID from the list of available networks, make sure the SSID appears in the Network name (SSID) field.
- If you clicked Add, enter the case-sensitive SSID of the access point or the ad hoc network to which you want the client adapter to associate in the Network name (SSID) field.

Step 9 Check the **This is a computer-to-computer (ad hoc mode) network; wireless access points are not used** check box at the bottom of the window if you are planning to operate the client adapter in an ad hoc network.

Step 10 Choose one of the following options from the Network Authentication drop-down list:

- **Open**—Enables your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. However, communication can occur only if the adapter's WEP key matches that of the access point. If your adapter is not using WEP, it will not attempt to authenticate to an access point that is using WEP and vice versa. This option is recommended if you want to use static WEP or EAP authentication without WPA.
- **Shared**—Enables your client adapter to authenticate and communicate only with access points that have the same WEP key. Cisco recommends that shared key authentication not be used because it presents a security risk.

Note Your client adapter's network authentication setting must match that of the access points with which it is to communicate. Otherwise, your client adapter may not be able to authenticate to them.

Note EAP-TLS does not work with shared key authentication because shared key authentication requires the use of a WEP key, and a WEP key is not set for EAP-TLS until after the completion of EAP authentication.

- **WPA**—Enables WPA, which enables your client adapter to associate to access points using WPA.
- **WPA-PSK**—Enables WPA pre-shared key (WPA-PSK), which enables your client adapter to associate to access points using WPA-PSK.

Note The WPA-None option is not supported for use with the CB21AG or PI21AG client adapter.

Note Refer to the "WPA" section on page E-4 for more information on WPA and WPA-PSK.

Step 11 Choose one of the following options from the Data encryption drop-down list:

- **Disabled**—Disables data encryption for your client adapter. This option is available only when Open or Shared has been selected for Network Authentication.
- **WEP**—Enables static or dynamic WEP for your client adapter. This option is recommended for use with open authentication.
- **TKIP**—Enables Temporal Key Integrity Protocol (TKIP) for your client adapter. This option is recommended for use with WPA and WPA-PSK unless the access point to which your client adapter will associate supports AES.
- **AES**—Enables the Advanced Encryption Standard (AES) encryption algorithm for your client adapter. This option provides a stronger encryption mechanism than TKIP and is therefore recommended for use with WPA and WPA-PSK, provided the access point to which your client adapter will associate supports AES.

Step 12 Follow the steps below to enter a static WEP key if you are planning to use static WEP.

Note If you are planning to use EAP-TLS or PEAP authentication, which uses dynamic WEP, go to Step 13.

a. Make sure the **The key is provided for me automatically** check box is unchecked.

b. Obtain the WEP key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in both the Network key and Confirm network key fields. Follow the guidelines below to enter a new static WEP key:

- WEP keys must contain the following number of characters:
  - –10 hexadecimal characters or 5 ASCII text characters for 40-bit keys

    Example: 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
  - –26 hexadecimal characters or 13 ASCII text characters for 128-bit keys

    Example: 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)

Note ASCII text WEP keys are not supported on Cisco Aironet 1200 Series Access Points, so you must enter hexadecimal characters if your client adapter will be used with these access points.

- Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.

c. In the Key index (advanced) field, choose the number of the WEP key you are creating (**1**, **2**, **3**, or **4**).

Note The WEP key must be assigned to the same number on both the client adapter and the access point (in an infrastructure network) or other clients (in an ad hoc network).

d. Click **OK** to save your settings and to add this SSID to the list of preferred networks (see Figure E-1). The configuration is complete for static WEP. The client adapter automatically attempts to associate to the network(s) in the order in which they are listed.

Step 13 If you enabled WPA-PSK, obtain the pre-shared key for the access point from your system administrator and enter it in both the Network key and Confirm network key fields. Follow the guidelines below to enter a pre-shared key:

- Pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- Your client adapter's pre-shared key must match the pre-shared key used by the access point with which you are planning to communicate.

Step 14 Check the **The key is provided for me automatically** check box if you are planning to use EAP-TLS or PEAP, which uses dynamic WEP keys.

Note This parameter is not available if you enabled WPA or WPA-PSK.

Step 15 Perform one of the following if you are planning to use EAP authentication:

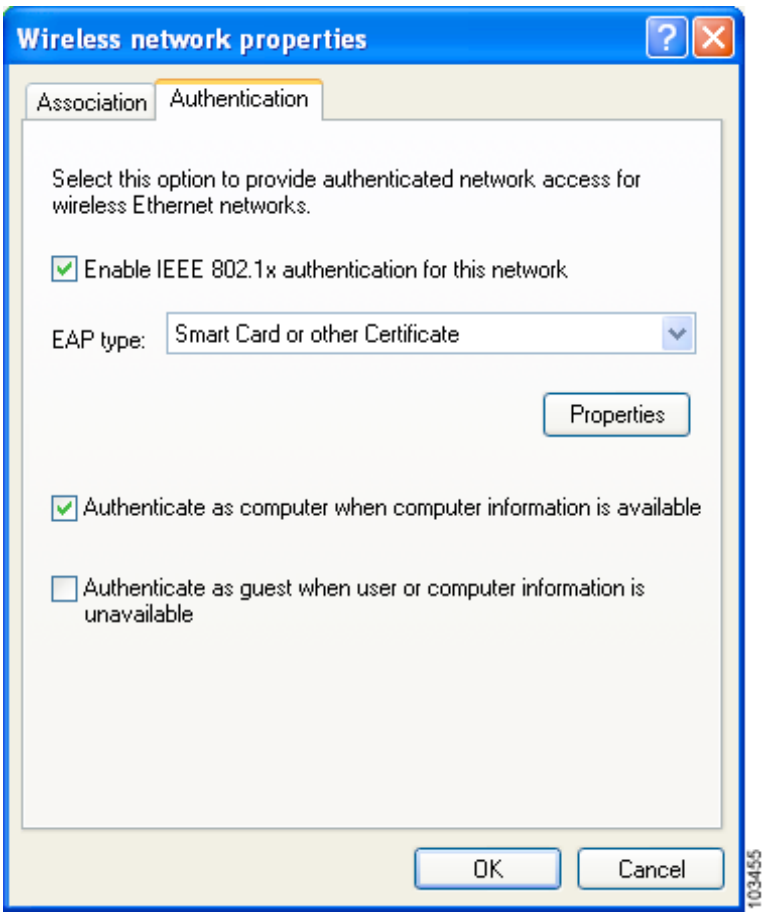
- If you are planning to use EAP-TLS authentication, follow the instructions in the "Enabling EAP-TLS Authentication" section on page E-10.
- If you are planning to use PEAP authentication, follow the instructions in the "Enabling PEAP Authentication" section on page E-13.

Enabling EAP-TLS Authentication

Follow the steps below to prepare the client adapter to use EAP-TLS authentication, provided you have completed the initial configuration.

Step 1 Click the **Authentication** tab on the Wireless Network Properties window. The following window appears (see Figure E-3).

Figure E-3 Wireless Network Properties Window (Authentication Tab)

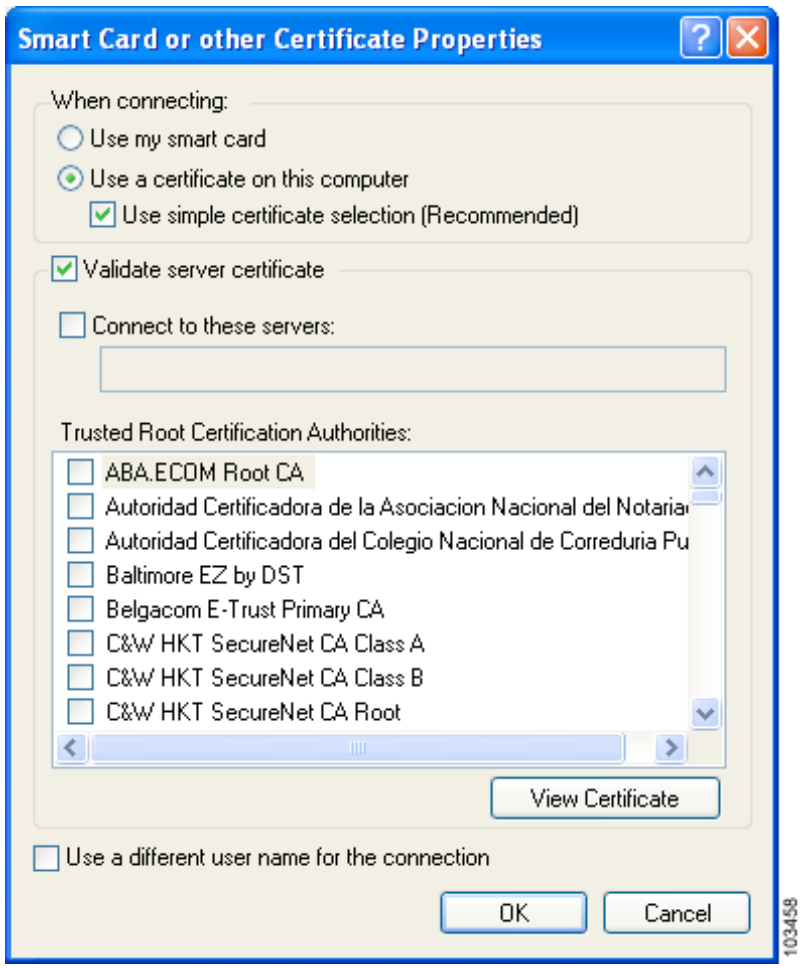


Step 2 Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.

Step 3 For EAP type, choose **Smart Card or other Certificate**.

Step 4 Click **Properties**. The Smart Card or other Certificate Properties window appears (see Figure E-4).

Figure E-4 Smart Card or other Certificate Properties Window



Step 5 Choose the **Use a certificate on this computer** option.

Step 6 Check the **Use simple certificate selection (Recommended)** check box.

Step 7 Check the **Validate server certificate** check box if server certificate validation is required.

Step 8 If you want to specify the name of the server to connect to, check the **Connect to these servers** check box and enter the server name in the field below.

Note If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.

Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

Step 9 In the Trusted Root Certification Authorities field, check the check box beside the name of the certificate authority from which the server certificate was downloaded.

Note If you leave all check boxes unchecked, you are prompted to accept a connection to the root certification authority during the authentication process.

Step 10 Click **OK** in each window to save your settings. The configuration is complete.

Step 11 If a pop-up message appears above the system tray informing you that you need to accept a certificate to begin the EAP authentication process, click the message and follow the instructions provided to accept the certificate.

Note You should not be prompted to accept a certificate for future authentication attempts. After you accept one, the same certificate is used subsequently.

Step 12 If a message appears indicating the root certification authority for the server's certificate, and it is the correct certification authority, click **OK** to accept the connection. Otherwise, click **Cancel**.

Step 13 If a message appears indicating the server to which your client adapter is connected, and it is the correct server to connect to, click **OK** to accept the connection. Otherwise, click **Cancel**.

The client adapter should now EAP authenticate.

Note Whenever the computer reboots and you enter your Windows username and password, the EAP authentication process begins automatically and the client adapter should EAP authenticate.

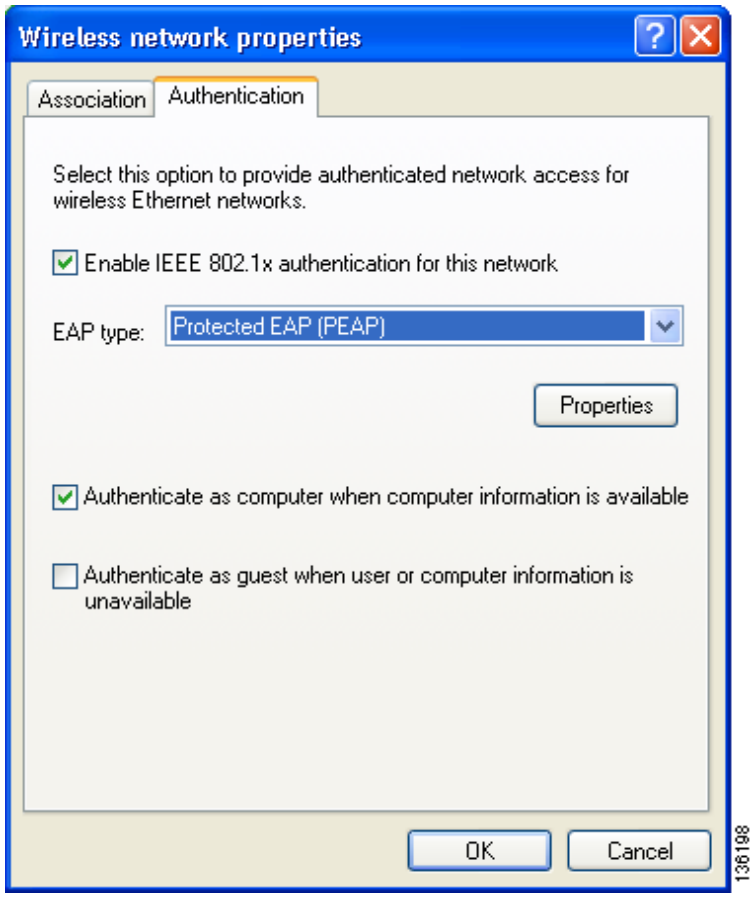
Step 14 To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication succeeded*.

Enabling PEAP Authentication

Follow the steps below to prepare the client adapter to use PEAP authentication, provided you have completed the initial configuration.

Step 1 Click the **Authentication** tab on the Wireless Network Properties window. The following window appears (see Figure E-5).

Figure E-5 Wireless Network Properties Window (Authentication Tab)



Step 2 Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.

Step 3 For EAP type, choose one of the following, depending on the software that is installed on your computer:

- **Protected EAP (PEAP)**—This option appears for PEAP (EAP-MSCHAP V2).
- **PEAP**—This option appears for PEAP (EAP-GTC).

Note PEAP (EAP-GTC) is not officially supported for CB21AG and PI21AG client adapters, but you may be able to use it successfully if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was previously installed on your computer and installed after Service Pack 1 for Windows XP.

Step 4 Perform one of the following:

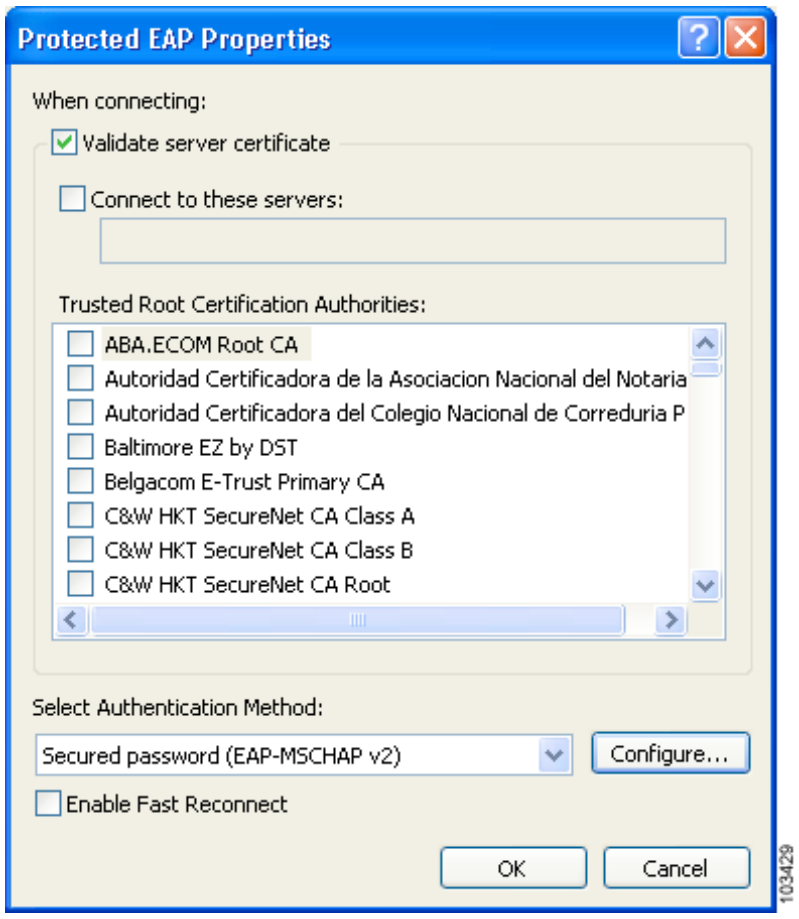
- If you chose Protected EAP (PEAP), follow the instructions in the "Enabling PEAP (EAP-MSCHAP V2)" section below.
- If you chose PEAP, follow the instructions in the "Enabling PEAP (EAP-GTC)" section on page E-16.

Enabling PEAP (EAP-MSCHAP V2)

Follow the steps below to enable PEAP (EAP-MSCHAP V2).

Step 1 Click **Properties**. The Protected EAP Properties window appears (see Figure E-8).

Figure E-6 Protected EAP Properties Window



Step 2 Check the **Validate server certificate** check box if server certificate validation is required (recommended).

Step 3 If you want to specify the name of the server to connect to, check the **Connect to these servers** check box and enter the appropriate server name in the field below.

Note If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.

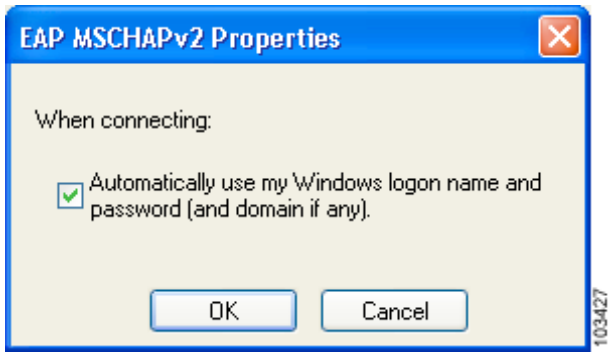
Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

Step 4 In the Trusted Root Certification Authorities field, choose the certificate authority from which the server certificate was downloaded.

Step 5 In the Select Authentication Method drop-down box, choose **Secured password (EAP-MSCHAP v2)**.

Step 6 Click **Configure**. The EAP MSCHAPv2 Properties window appears (see Figure E-7).

Figure E-7 EAP MSCHAPv2 Properties Window



Step 7 Make sure the **Automatically use my Windows logon name and password (and domain if any)** check box is checked.

Step 8 Click **OK** in each window to save your settings. The configuration is complete.

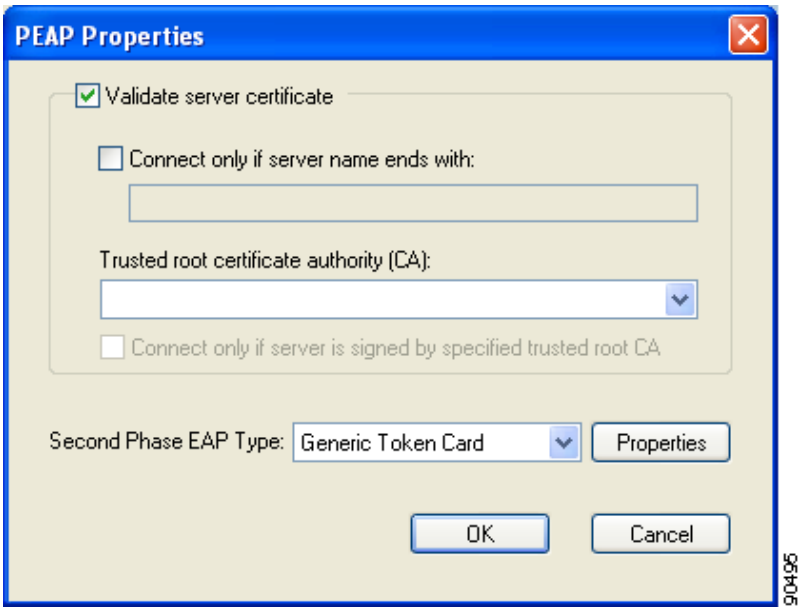
Step 9 The EAP authentication process begins automatically, and the client adapter should EAP authenticate using your Windows credentials. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication succeeded*.

Enabling PEAP (EAP-GTC)

Follow the steps below to enable PEAP (EAP-GTC).

Step 1 Click **Properties**. The PEAP Properties window appears (see Figure E-8).

Figure E-8 PEAP Properties Window



Step 2 Check the **Validate server certificate** check box if server certificate validation is required (recommended).

Step 3 If you want to specify the name of the server to connect to, check the **Connect only if server name ends with** check box and enter the appropriate server name suffix in the field below.

Note If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.

Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

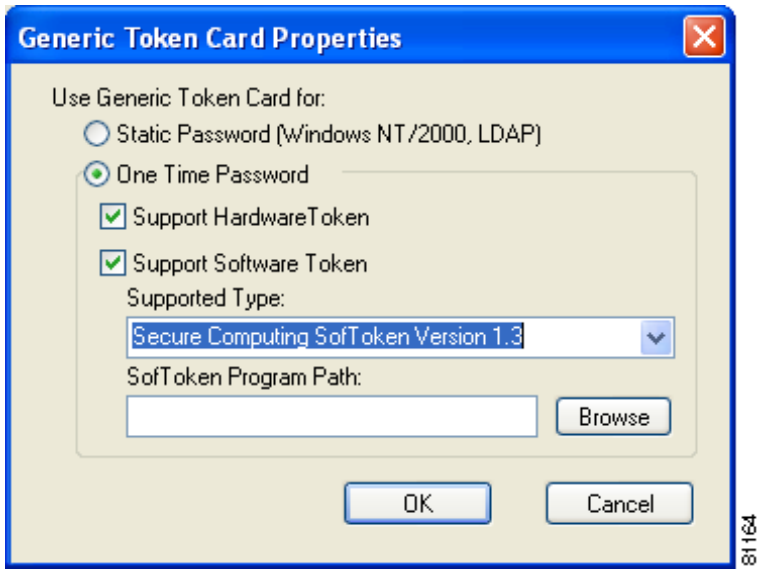
Step 4 Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate authority (CA) field. If necessary, click the arrow on the drop-down menu and choose the appropriate name.

Note If you leave this field blank, you are prompted to accept a connection to the root certification authority during the authentication process.

Step 5 Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.

Step 6 Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties window appears (see Figure E-9).

Figure E-9 Generic Token Card Properties Window



Step 7 Choose either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.

Step 8 Perform one of the following:

- If you chose the **Static Password (Windows NT/2000, LDAP)** option in Step 7, go to Step 9.
- If you chose the **One Time Password** option in Step 7, check one or both of the following check boxes to specify the type of tokens that will be supported for one-time passwords:
  - **Support Hardware Token**—A hardware token device obtains the one-time password. You must use your hardware token device to obtain the one-time password and enter the password when prompted for your user credentials.
  - **Support Software Token**—The PEAP supplicant works with a software token program to retrieve the one-time password. You have to enter only the PIN, not the one-time password. If you check this check box, you must also choose from the Supported Type drop-down box the software token software that is installed on the client (such as Secure Computing SofToken Version 2.1, Secure Computing SofToken II 2.0, or RSA SecurID Software Token 2.5), and if Secure Computing SofToken Version 2.1 is selected, you must find the software program path using the Browse button.

Note The SofToken Program Path field is unavailable if a software token program other than Secure Computing SofToken Version 2.1 is selected.

Step 9 Click **OK** in each window to save your settings. The configuration is complete.

Step 10 Refer to Chapter 6 of the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* (OL-1394-07 or later) for instructions on authenticating using PEAP (EAP-GTC).

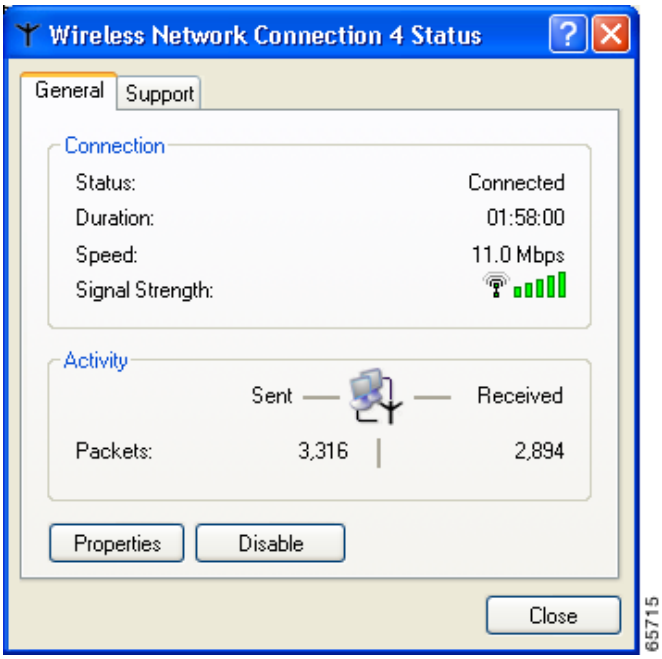
Associating to an Access Point Using Windows XP

Windows XP causes the client adapter's driver to automatically attempt to associate to the first network in the list of preferred networks (see Figure E-1). If the adapter fails to associate or loses association, it automatically switches to the next network in the list of preferred networks.The adapter does not switch networks as long as it remains associated to the access point. To force the client adapter to associate to a different access point, you must choose a different network from the list of available networks (and click **Configure** and **OK**).

Viewing the Current Status of Your Client Adapter

To view the status of your client adapter, click the icon of the two connected computers in the Windows system tray. The Wireless Network Connection Status window appears (see Figure E-10).

Figure E-10 Wireless Network Connection Status Window



Performing a Site Survey

This appendix explains how the site survey utility can be used when conducting a site survey. The following topics are covered in this appendix:

- Overview, page F-2
- Opening the Site Survey Utility, page F-3
- Selecting the Client Adapter, page F-3
- Using the Associated AP Status Tab, page F-4
- Using the AP Scan List Tab, page F-8
- Finding the Version of the Site Survey Utility, page F-15
- Accessing Online Help, page F-15
- Exiting the Site Survey Utility, page F-15
- Uninstalling the Site Survey Utility, page F-15

Overview

Note This appendix applies only to people who are responsible for conducting a site survey to determine the best placement of infrastructure devices within a wireless network.

Note The site survey utility is available in Install Wizard 2.0 and later.

The site survey utility can assist you in conducting a site survey. The utility operates at the RF level and is used to determine the best placement and coverage (overlap) for your network's infrastructure devices. During a site survey, the current status of the network is read from the client adapter, and the status display is updated four times per second so you can accurately gauge network performance. The feedback that you receive can help you to eliminate areas of low RF signal levels that can result in a loss of connection between the client adapter and its associated access point (or other infrastructure device).

The site survey utility operates in a passive mode. That is, it does not initiate any RF network traffic; it simply listens to the traffic that the client adapter hears and displays the results.

Guidelines

Keep the following guidelines in mind when preparing to perform a site survey:

- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.

Additional Information

Also consider the following operating and environmental conditions when performing a site survey:

- **Data rates**—Sensitivity and range are inversely proportional to data bit rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data increases.
- **Antenna type and placement**—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
- **Physical environment**—Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- **Obstructions**—A physical obstruction such as metal shelving or a steel pillar can hinder the performance of wireless devices. Avoid placing these devices in a location where a metal barrier is between the sending and receiving antennas.
- **Building materials**—Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks, and metal or steel construction is a barrier to radio signals.

Note Refer to the hardware installation guide for your infrastructure device for additional information on factors affecting placement.

Opening the Site Survey Utility

To open the site survey utility, choose **Start** > **Programs** > **Cisco Aironet** > **Aironet Site Survey Utility**.

Note If you specified a different program folder during installation, you must access the site survey utility from that folder.

Note The site survey utility is installed on your computer only if you checked the Install Site Survey Utility check box during the installation of the client adapter software. If you did not check this check box and want to use the site survey utility, uninstall the client adapter software and reinstall it, making sure to check the site survey check box.

Selecting the Client Adapter

Note The site survey utility is supported for use with only CB21AG and PI21AG client adapters.

When the site survey utility starts, it scans for client adapters. If only one adapter is detected, it is selected automatically. However, if the utility detects multiple adapters or no adapters, the Select Adapter window appears (see Figure F-1).

Note You can manually open this window at any time to select a different client adapter. Simply choose **Select Adapter** from the site survey utility's Action drop-down menu.

Figure F-1 Site Survey Utility - Select Adapter Window

Follow these steps to select the desired client adapter.

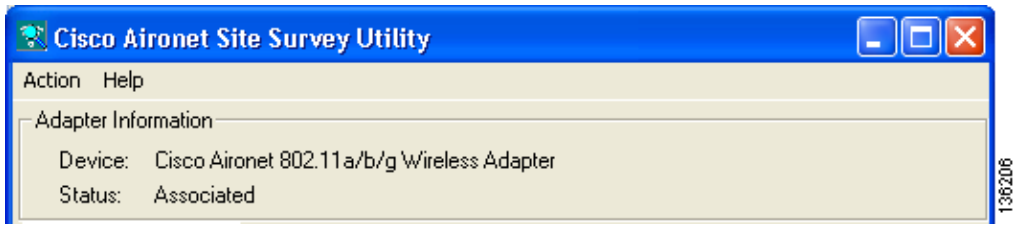
Step 1 If you want to be able to choose client adapters that are installed but not physically present in your computer, check the **List installed devices even if not present in system** check box.

Step 2 From the Select a Network Adapter list, select the client adapter that you want to use with the site survey utility.

Note Click **Refresh** to update the list of available client adapters (for instance, after an adapter has been ejected or inserted).

Step 3 Click **OK** to save your selection and exit the Select Adapter window. The top of the site survey utility's main window (see Figure F-2) shows the client adapter that is being used with the utility and its current association status (Associated, Not Associated, or Device Not Present).

Figure F-2 Site Survey Utility - Top of Main Window



Using the Associated AP Status Tab

You can perform two functions from the Associated AP Status tab:

- Specify display units, page F-4
- View the access point's status, page F-5

Follow the instructions on the pages indicated to perform these functions.

Specifying Display Units

The **Display in percent** check box at the bottom of the Associated AP Status tab enables you to specify how display units are shown.

Note This check box is available in site survey utility 1.1 and later.

- Unchecking this check box causes the signal strength and noise level to be shown in decibels with respect to milliwatts (dBm) and the signal-to-noise ratio to be shown in decibels (db). This option, which is the default value, provides a more accurate representation of the data being presented than the percentage option.
- Checking this check box causes the signal strength, signal quality or beacons received, and overall link quality to be shown as a percentage.

Viewing the Access Point's Status

The Associated AP Status tab shows the status of the access point to which your client adapter is associated. Figure F-3 shows the tab with display units shown in dBm, and Figure F-4 shows the tab with display units shown as a percentage.

Figure F-3 Site Survey Utility - Associated AP Status Tab (with Display Units in dBm)

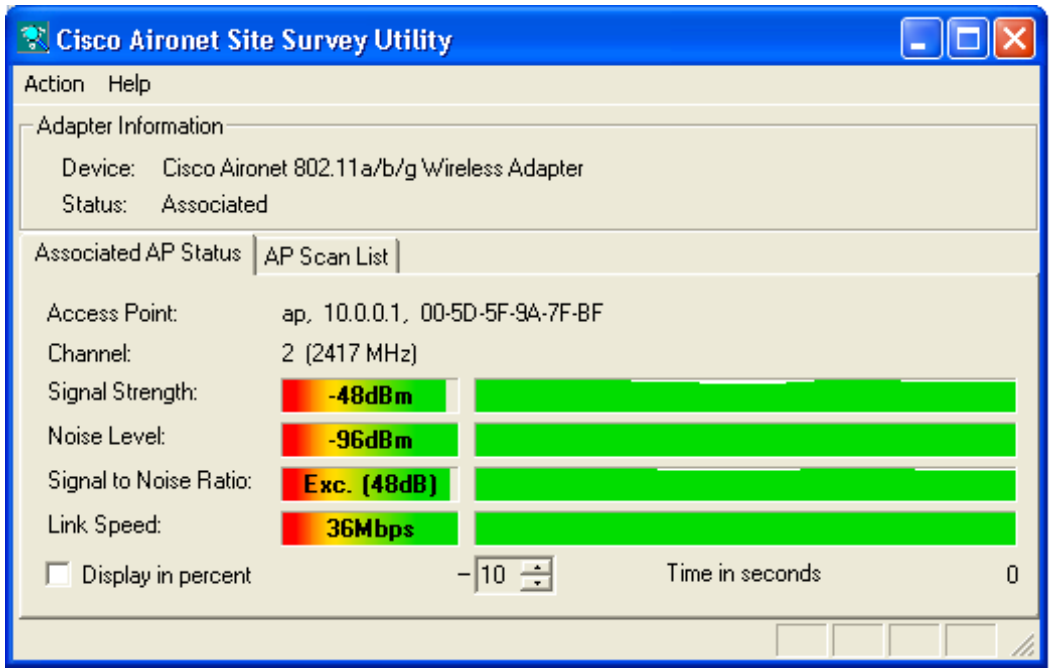


Figure F-4 Site Survey Utility - Associated AP Status Tab (with Display Units as a Percentage)

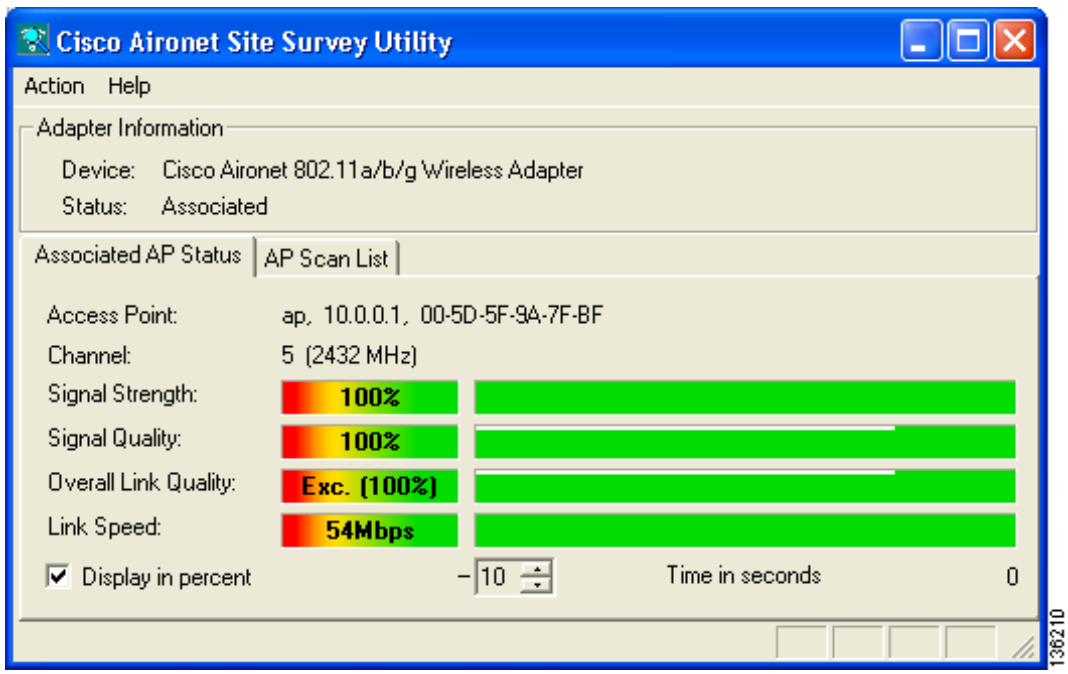


Table F-1 interprets the information that is displayed on the Associated AP Status tab.

Note The trend graphs to the right of the smaller bar graphs provide a graphical representation of activity in the past 10 to 60 seconds. The height of an individual trend graph is proportional to the width of its corresponding bar graph. The time is displayed as a negative value to indicate that the data is older at the left edge of the graph than at the right. Use the up and down arrows to select the desired number of seconds from -10 through -60. The default value is -10.

Table F-1 Site Survey Utility - Associated AP Status

Associated AP Status Parameter	Description
Access Point	The access point to which your client adapter is associated. This field may show the access point's name, IP address, and MAC address. **Note** This information is shown only if the access point was configured with a name and/or IP address, Aironet Extensions are enabled (on access points running Cisco IOS release 12.2(4)JA or greater), and the access point transmits this information. **Note** This field shows up to 15 characters for the access point name although the name may be longer. **Note** If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0. **Note** This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.
Channel	The channel and radio frequency that the access point is currently using for communications. **Value:** Dependent on radio band and regulatory domain
Signal Strength	The signal strength of the most recently received packets. The higher the value and the wider the bar graph, the stronger the signal. The trend graph to the right of the bar graph provides a visual interpretation of the signal strength over time. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest). **Range:** –95 to –45 dBm or 0 to 100%

Table F-1 Site Survey Utility - Associated AP Status (continued)

Associated AP Status Parameter	Description
Noise Level	The level of background radio frequency energy. The lower the value and the wider the bar graph, the less background noise present. The trend graph to the right of the bar graph provides a visual interpretation of the level of background noise over time. Differences in background noise level are indicated by the following colors: green (low noise), yellow (middle of the range), and red (high noise). **Range:** –45 to –95 dBm **Note** This parameter appears only if the Display in Percent check box is unchecked.
Signal Quality	The signal quality of the most recently received packets. The higher the value and the wider the bar graph, the clearer the signal. The trend graph to the right of bar graph provides a visual interpretation of the signal quality over time. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality). **Range:** 0 to 100% **Note** This parameter appears only if the Display in Percent check box is checked.
Beacons Received	The percentage of beacon packets received from the access point versus those expected to be received. The higher the value and the wider the bar graph, the clearer the signal. The trend graph to the right of bar graph provides a visual interpretation of the signal clarity over time. Differences in signal clarity are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality). **Example:** The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%. **Range:** 0 to 100% **Note** This parameter appears only if the Display in Percent check box is checked and the client adapter does not provide a signal quality value.

Table F-1 Site Survey Utility - Associated AP Status (continued)

Associated AP Status Parameter	Description
Signal to Noise Ratio	The difference between the signal strength and the noise level. The higher the value and the wider the bar graph, the better the client adapter's ability to communicate with the access point. The trend graph to the right of the bar graph provides a visual interpretation of the signal-to-noise ratio over time. Differences in the client adapter's ability to communicate are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality). **Range:** Poor, Fair, Good, Excellent; 0 to 50 dB **Note** This parameter appears only if the Display in Percent check box is unchecked.
Overall Link Quality	A combination of signal strength and signal quality. The higher the value and the wider the bar graph, the better the client adapter's ability to communicate with the access point. The trend graph to the right of the bar graph provides a visual interpretation of the overall link quality over time. Differences in quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality). **Value:** Poor, Fair, Good, Excellent; 0 to 100% **Note** This parameter appears only if the Display as Percent check box is checked.
Link Speed	The site survey utility monitors transmitted network traffic, and the link speed reflects the current transmit rate of data packets. The trend graph provides a visual interpretation of the packet transmit rate over time. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest). **Value:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps, depending on radio band

Using the AP Scan List Tab

You can perform four functions from the AP Scan List tab:

- View the AP scan list, page F-9
- Pause the AP scan list, page F-11
- View AP details, page F-12
- Generate an AP scan log file, page F-14

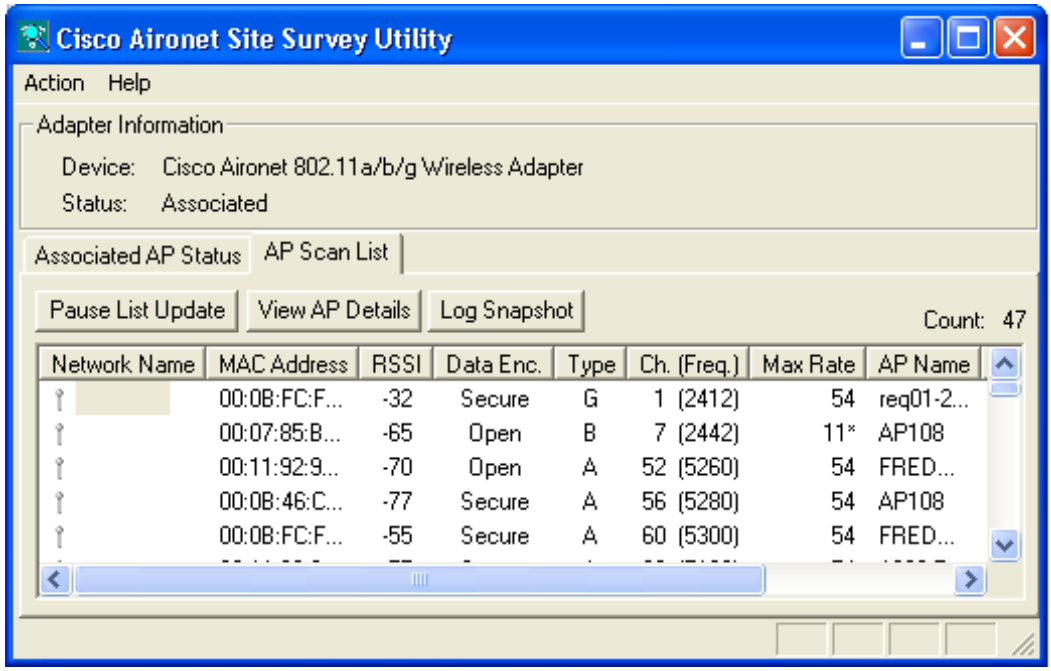
Follow the instructions on the pages indicated to perform these functions.

Viewing the AP Scan List

Your client adapter can detect nearby access points by the beacon signals that the access points continually transmit. The AP scan list displays a continuously updated list of the access points detected by your client adapter as well as the information contained in their beacons.

To view the AP scan list, click the **AP Scan List** tab. The AP scan list appears (see Figure F-5).

Figure F-5 Site Survey Utility - AP Scan List



To view the entire list of access points and all their information, perform one of the following:

- Click the resize tab in the lower right corner of the main window and drag it until the window reaches the desired size.
- Use the vertical and horizontal scroll bars.
- Click the middle button in the top right corner of the window.

Table F-2 interprets the information that is displayed in the AP scan list.

Note The AP Detailed Information window provides details for many of the parameters listed in Table F-2. See the "Viewing AP Details" section on page F-12 for additional information.

Table F-2 Site Survey Utility - AP Scan List

AP Scan List Parameter	Description
Count	The number of rows, or access points, in the scan list. **Note** This parameter appears above the AP scan list and to the left.
Network Name	The network name, or service set identifier (SSID), indicates the name of an available wireless network. The icon to the left of the SSID provides information on link status.

Icon	Description
	An available wireless network.
	The wireless network to which your client adapter is currently associated.

Note The SSID of a Cisco IOS access point appears in the list of available networks only if a Guest Mode SSID is enabled or the Broadcast SSID in Beacon option is selected. Refer to the software configuration guide for your access point for additional information.

MAC Address	The access point's MAC address. **Note** This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.
RSSI	The received signal strength indicator (RSSI) is a measure of signal strength in decibels with respect to milliwatts (dBm).
Data Encryption	Indicates whether the data exchanged with this access point is encrypted. **Value:** Secure or Open

Value	Description
Secure	The data exchanged with this access point is encrypted.
Open	The data exchanged with this access point is unencrypted.

Type	The IEEE 802.11 standard that describes the access point's radio band. **Value:** A, B, or G
Channel (Frequency)	The channel and radio frequency that the access point is currently using for communications. **Value:** Dependent on radio band and regulatory domain
Max Rate	The maximum rate at which the access point can transmit data.

Table F-2 Site Survey Utility - AP Scan List (continued)

AP Scan List Parameter	Description	
AP Name	The access point's name. It is shown only if the access point was configured with a name, Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later), and the access point transmits this information. **Note** This field shows up to 15 characters although the name of the access point may be longer.	
CCX	The version of Cisco Compatible Extensions (CCX) supported by the access point. It is shown only if the access point transmits this information. **Value:** 1, 2, 3, or 4	
Other Information	A list of miscellaneous values that may appear depending on the access point's current status and the information that it transmits. **Values:** Ad-Hoc, Power, Qos, RM-Normal, RM-Source, and Ssidl	
	Value	**Description**
	Ad-Hoc	Indicates that the device is not an access point but another client adapter operating in ad hoc mode.
	Power	Indicates whether the access point can limit the transmitting power of the client adapter. If so, the power limit is also shown in milliwatts (mW).
	Qos	Indicates whether the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.
	RM-Normal RM-APScan RM-CliWlk	Indicates whether the access point is using radio management. If so, a value of 1 indicates normal status, 2 indicates AP radio scan, and 3 indicates client walkabout. Any other value appears as RM-State:*xxx*, where *xxx* represents a numerical value.
	RM-Source	Indicates whether the access point is using radio management extensions and displays the MAC address of the radio management source (for example, RM-Source: 00-07-85-B4-04-9F).
	Ssidl	Indicates the number of advertised alternate SSIDs (for example, Ssidl:2).

Pausing the AP Scan List

The AP scan list is updated continually. To pause the current list, click **Pause List Update** above the AP scan list.

Note Clicking this button again resumes the list update.

Viewing AP Details

To view details for a particular access point in the AP scan list, select the desired network name in the scan list and click **View AP Details**. The AP Detailed Information window appears (see Figure F-6).

Note You can also open the AP Detailed Information window by double-clicking in the first column of the desired row.

Figure F-6 Site Survey Utility - AP Detailed Information Window

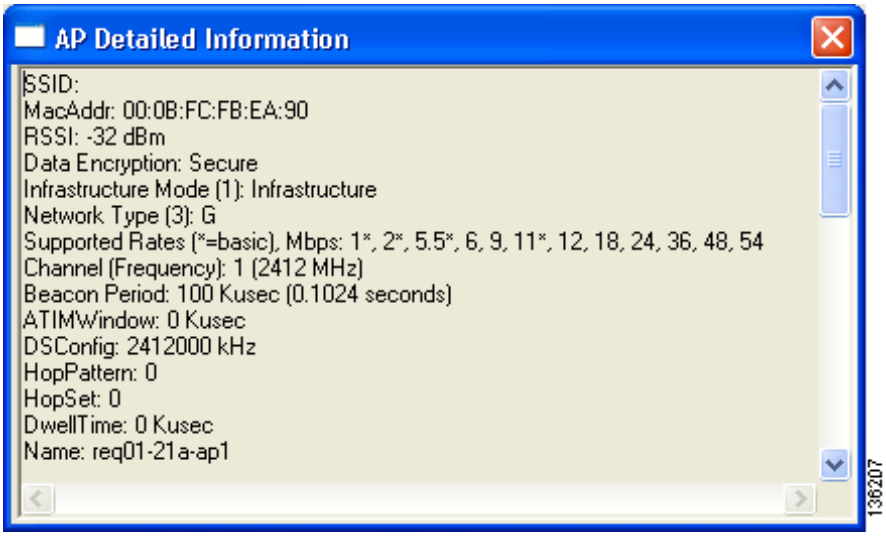


Table F-3 interprets the information that is displayed in the AP Detailed Information window.

Note The AP Detailed Information window contains tegxt summaries of all the information elements present in the access point's beacon or probe response. As a result, the window may contain different information than that described in Table F-3.

Table F-3 Site Survey Utility - AP Detailed Information

Detailed Information Parameter	Description
SSID	The network name, or service set identifier (SSID), indicates the name of the access point's wireless network.
MAC Address	The access point's MAC address. **Note** This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.

Table F-3 Site Survey Utility - AP Detailed Information (continued)

Detailed Information Parameter	Description
RSSI	The received signal strength indicator (RSSI) is a measure of signal strength in decibels with respect to milliwatts (dBm).
Data Encryption	Indicates whether the data exchanged with this access point is encrypted. **Value:** Secure or Open
Infrastructure Mode	Indicates whether the device is an access point operating in infrastructure mode or another client adapter operating in ad hoc mode. **Value:** Infrastructure or Ad-Hoc
Network Type	The IEEE 802.11 standard that describes the access point's radio band. **Value:** A, B, or G
Supported Rates	The rate at which the access point is capable of transmitting and receiving data packets. **Value:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Channel (Frequency)	The channel and radio frequency that the access point is currently using for communications. **Value:** Dependent on radio band and regulatory domain
Beacon Period	The amount of time between access point beacons in Kilomicroseconds (Kμsec). **Note** One Kμsec equals 1,024 microseconds.
ATIMWindow	Announcement traffic information message (ATIM) window. The brief time period immediately following the transmission of each beacon in an ad hoc network. This value is expressed in Kilomicroseconds (Kμsec). **Note** One Kμsec equals 1,024 microseconds. **Note** This parameter's value is 0 when the device is operating in infrastructure mode.
DSConfig	The frequency of the selected channel. **Range:** 2,412,000 to 2,484,000 kHz (802.11b/g); 5,000,000 to 6,000,000 kHz (802.11a)
HopPattern	The hop pattern used to determine the hop sequence.
HopSet	A set of patterns used to determine the hop sequence.
DwellTime	The maximum amount of time that the access point should remain on a channel. This value is expressed in Kilomicroseconds (Kμsec). **Note** One Kμsec equals 1,024 microseconds.
Name	The access point's name. It is shown only if the access point was configured with a name, Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later), and the access point transmits this information. **Note** This field shows up to 15 characters although the name of the access point may be longer.

Generating an AP Scan Log File

To enter the current contents of the AP scan list into a log file that can be saved to your computer's hard drive, click **Log Snapshot**. The "Logged current AP Scan List" message appears below the scan list, and the log file is saved as a text file in the same directory as the site survey utility. The default location is C:\Program Files\Cisco Aironet (unless you specified a different location during installation).

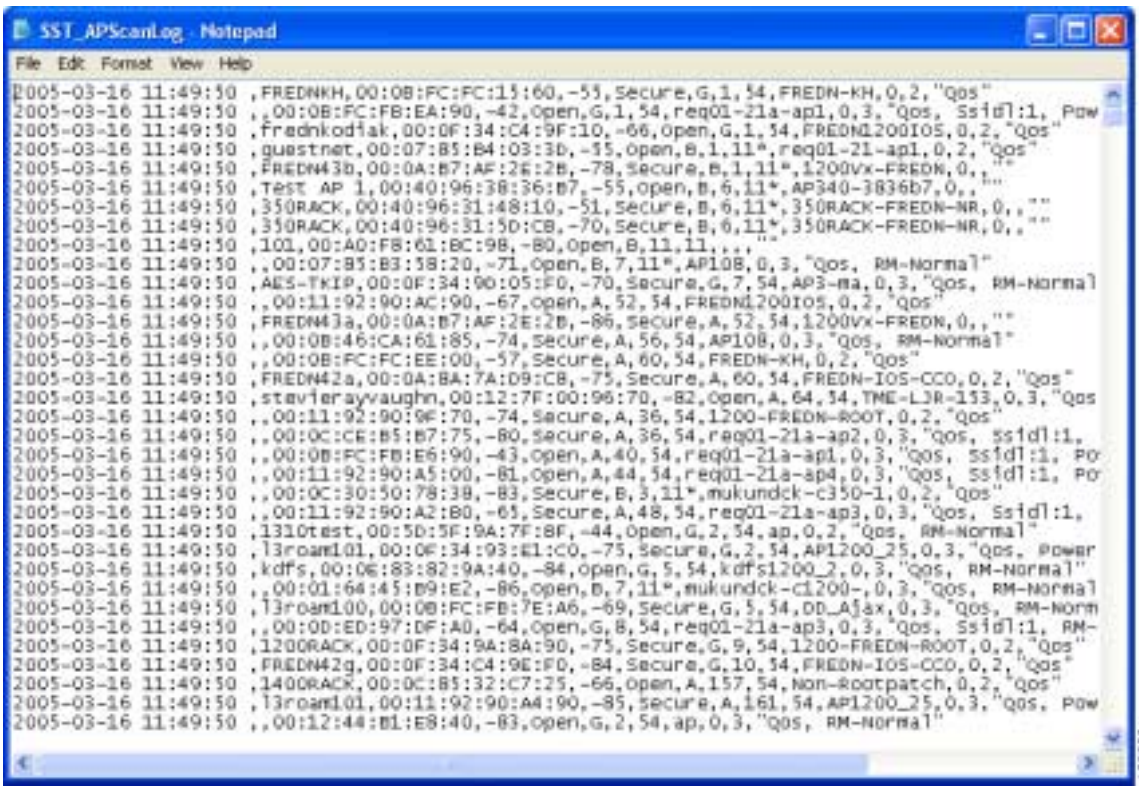
Note If the AP scan list is paused when you click Log Snapshot, the currently displayed data (not the latest available data) is added to the log.

Note Each time you click **Log Snapshot**, the new scan list is written at the end of the existing log file.

To view the log file, find and open the file (SST_APScanLog.txt) using Windows Explorer. The log file appears (see Figure F-7).

Note The log file can be viewed by a spreadsheet or database program (such as Microsoft Excel). It is written in comma-separated values (CSV) format. Therefore, if the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.

Figure F-7 Site Survey Utility - Log File

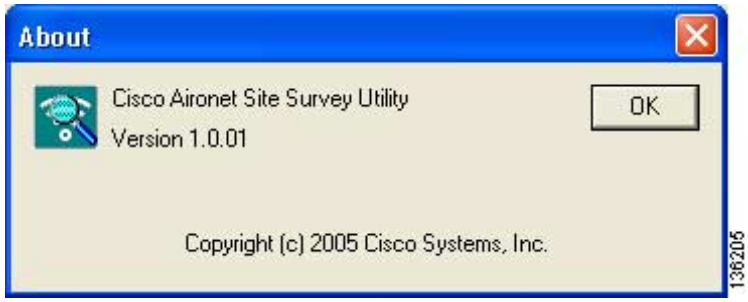


The log entries are time-stamped and appear in ASCII text. Each line represents a different access point.

Finding the Version of the Site Survey Utility

To find the current version of the site survey utility, choose **About** from the Help drop-down menu. The About window appears (see Figure F-8).

Figure F-8 Site Survey Utility - About Window



Accessing Online Help

To access the site survey utility's online help, choose **Contents** from the Help drop-down menu.

Exiting the Site Survey Utility

To exit the site survey utility, perform one of the following:

- Click the **X** in the top right corner of the main window.
- Choose **Exit** from the Action drop-down menu.

Uninstalling the Site Survey Utility

Uninstalling the client adapter software also uninstalls the site survey utility. Refer to the "Uninstalling the Client Adapter Software" section on page 9-6 for instructions.

16-QAM Quadrate amplitude modulation. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 24 and 36 Mbps.

64-QAM Quadrate amplitude modulation. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 48 and 54 Mbps.

802.1X Also called *802.1X for 802.11*. 802.1X is the standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

802.11 The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) 2.4-GHz wireless LANs.

802.11a The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see UNII, UNII 1, and UNII 2) and provides four channels per 100 MHz of bandwidth.

802.11b The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps 2.4-GHz wireless LANs.

802.11g The IEEE standard that specifies carrier sense media access control and physical layer specifications for 54-Mbps 2.4-GHz wireless LANs.

802.11i The IEEE standard that defines security standards for wireless LANs. It specifies encryption, authentication, and key management strategies for wireless data and system security. It includes the TKIP and AES-CCMP data-confidentiality protocols.

A

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

ad hoc network A wireless network composed of stations without access points.

AES-CCMP Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES-CCMP is the encryption protocol in the 802.11i standard.

alphanumeric A set of characters that contains both letters and numbers.

associated A station is configured properly to enable it to wirelessly communicate with an access point.

B

bandwidth Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant power loss.

BPSK Binary phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 1 Mbps.

broadcast key rotation A security feature for use with dynamic WEP keys. If your client adapter uses LEAP, EAP-FAST, EAP-TLS, or PEAP authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

CCKM Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.

CKIP Cisco Key Integrity Protocol. Cisco’s WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.

client A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

CRC Cyclic redundancy check. A method of checking for errors in a received packet.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and the more acute the angle of coverage.

DHCP Dynamic Host Configuration Protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

DSSS Direct-sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

duplicate packets Packets that were received twice because an acknowledgement got lost and the sender retransmitted the packet.

E

EAP Extensible Authentication Protocol. EAP is the protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

EAP-FAST Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling. An 802.1X authentication type that is available for use with Windows 2000 and XP. With EAP-FAST, a username, password, and PAC are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to enable computers to share a network and operates at 10, 100, or 1000 megabits per second (Mbps), depending on the physical layer used.

F

file server A repository for files so that a local area network can share files, mail, and programs.

fragmentation threshold The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 64 to 2312 bytes.

full duplex A means of communication whereby each node receives and transmits simultaneously (two-way). See also half duplex.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

H

half duplex A means of communication whereby each node receives and transmits in turn (one-way). See also full duplex.

hexadecimal A set of characters consisting of ten numbers and six letters (0-9, A-F, and a-f).

I

IEEE Institute of Electrical and Electronics Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

infrastructure The wired Ethernet network.

infrastructure device A device (such as an access point, bridge, or base station) that connects client adapters to a wired LAN.

IP address The Internet Protocol address of a station.

IP subnet mask The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

IPX Internetwork Packet Exchange. The NetWare network layer protocol used for transferring data from servers to workstations.

L

LEAP LEAP, or *EAP-Cisco Wireless*, is an 802.1X authentication type. With LEAP, a username and password are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.

M

MAC address The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.

MIC Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multicast packets Packets transmitted to multiple stations.

multipath The echoes created as a radio signal bounces off of physical objects.

O

OFDM Orthogonal frequency division multiplexing. A multicarrier modulation method for broadband wireless communications.

overrun packets Packets that were discarded because the access point had a temporary overload of packets to handle.

P

PAC Protected access credentials. Credentials that are either automatically or manually provisioned and used to perform mutual authentication with the RADIUS server during EAP-FAST authentication. PACs are created by the Cisco Secure ACS server and are identified by an ID. The user obtains his or her own copy of the PAC from the server, and the ID links the PAC to the profile created in ADU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported onto the client device.

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

QoS Quality of service. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QPSK Quadruple phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 2 Mbps.

R

radio channel The frequency at which a radio operates.

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio frequency. A generic term for radio-based technology.

roaming A feature of some access points that enables users to move through a facility while maintaining an unbroken connection to the LAN.

RTS threshold The packet size at which an access point issues a request to send (RTS) before sending the packet.

S

spread spectrum A radio transmission technology that spreads data over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

SSID Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

TKIP Temporal Key Integrity Protocol. Also referred to as *WEP key hashing*. A security feature that defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.

transmit power The power level of radio transmission.

U

unicast packets Packets transmitted in point-to-point communication.

UNII Unlicensed National Information Infrastructure. An FCC regulatory domain for 5-GHz wireless devices. UNII bands are 100 MHz wide and divided into four channels when using 802.11a OFDM modulation.

UNII 1 A UNII band dedicated to in-building wireless LAN applications. UNII 1 is located at 5.15 to 5.25 GHz and allows for a maximum transmit power of 40 mW (or 16 dBm) with an antenna up to 6 dBi. UNII 1 regulations require a nonremovable, integrated antenna.

UNII 2 A UNII band dedicated to in-building wireless LAN applications. UNII 2 is located at 5.25 to 5.35 GHz and allows for a maximum transmit power of 200 mW (or 23 dBm) with an antenna up to 6 dBi. UNII 2 regulations allow for an auxiliary, user-installable antenna.

UNII 3 A UNII band dedicated to wireless LAN applications. UNII 3 is located at 5.725 to 5.825 GHz and allows for a maximum transmit power of 1 Watt (or 30 dBm) with an antenna up to 6 dBi. UNII 3 regulations allow for an auxiliary, user-installable antenna.

V

VLAN A switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

W

WDS Wireless domain services (WDS). An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP Wired equivalent privacy. An optional security mechanism defined within the 802.11 standard designed to protect your data as it is transmitted through your wireless network by encrypting it through the use of encryption keys.

WMM Wi-Fi Multimedia. WMM is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). It specifically supports priority tagging and queuing.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access. A standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard’s ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.

WPA2 Wi-Fi Protected Access 2. The next generation of Wi-Fi security. It is the Wi-Fi Alliance’s implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.

Numerics

802.11 Authentication Mode parameter 5-12
802.11b preamble, status of 7-11
802.11b Preamble parameter 5-9
802.11 mode, in ASTU 8-5
802.1X
  authentication types
    in ADU 5-15 to 5-17
    in Windows XP E-3
  defined 5-15, E-3
802.1x EAP Type parameter 5-28, 5-31, 5-40, 5-42, 5-46, 5-49
802.1x option 5-28, 5-31, 5-40, 5-42, 5-46, 5-49

A

About Aironet Desktop Utility, ADU menu option 9-8
About window
  in ADU 9-8
  in site survey utility F-15
access point
  CCX version supported F-11
  channel, in site survey utility F-6, F-10, F-13
  currently associated to 7-9, 8-11
  data rates, in site survey utility F-13
  frequency, in site survey utility F-6, F-10, F-13
  in wireless infrastructure 1-6
  IP address
    in ADU 7-9
    in ASTU 8-11
    in site survey utility F-6
  MAC address
    in ADU 7-9
    in site survey utility F-6, F-10, F-12
  maximum transmit data rate, in site survey utility F-10
  mismatches 7-14
  name
    in ADU 7-9
    in ASTU 8-11
    in site survey utility F-6, F-11, F-13
  problems associating to 10-10
  radio band, in site survey utility F-10, F-13
  role in wireless network 1-5
  security settings 5-20 to 5-24
Access Point 1 through 4 parameters 5-13
access points
  associating to in Windows XP E-18
  number displayed in site survey utility F-10
  preferred, setting 5-13
  reporting those that fail LEAP authentication 5-19, 5-23
  viewing details in site survey utility F-12 to F-13
  viewing status in site survey utility F-5 to F-8
ACK frames 7-14
Action drop-down menu
  in ADU 6-10, 9-7
  in site survey utility F-3, F-15
Activate button 4-5, 4-9
Adapter Information
  button 9-8
  window 9-8
ad hoc mode, in site survey utility F-11
ad hoc network
  defined E-6
  selecting in ADU 5-9

selecting in Windows XP E-7
setting wireless mode 5-10
wireless LAN configuration 1-5
ADU
See Aironet Desktop Utility (ADU)
Advanced button 7-6
advanced parameters
described 5-2
setting 5-6 to 5-13
Advanced Statistics
button 7-13
window 7-13
Advanced Status window 7-7
AES, status of 7-6, 7-7
AES-CCMP, with WPA2 5-18
AES option, in Windows XP E-8
Aironet Desktop Utility (ADU)
accessing help 9-9
described 1-4
exiting 9-7
feature comparison to Windows XP 3-17 to 3-18
finding version 9-8
icon, using to open ADU 9-7
opening 9-7
Profile Management windows, overview 5-2
status and statistics tools
overview 7-2
setting parameters 7-2 to 7-3
using 7-4 to 7-15
Aironet Desktop Utility Help, ADU menu option 9-9
Aironet System Tray Utility (ASTU)
accessing help 8-5
described 1-4
exiting 8-6
icon 8-2 to 8-3, 9-7
opening 8-6
overview 8-2
pop-up menu 8-5 to 8-11
selecting the active profile 8-8 to 8-9
setting preferences 8-6 to 8-7
specifying pop-up menu options 8-7
Tool Tip window 8-3 to 8-5
using 8-1 to 8-11
using to open ADU 8-6
using to open troubleshooting utility 8-6
Aironet System Tray Utility Preferences window 8-6
Allow Association to Mixed Cells parameter
setting with EAP-FAST 5-37
setting with EAP-TLS 5-41
setting with LEAP 5-30
setting with PEAP (EAP-GTC) 5-45
setting with PEAP (EAP-MSCHAP V2) 5-48
setting with static WEP 5-26
Allow Automatic PAC Provisioning for this Profile parameter 5-33
Always Do User Authentication parameter 5-41
antenna
assembling 3-5 to 3-6
described 1-3
gains
IEEE 802.11a D-4
IEEE 802.11b D-4
IEEE 802.11g D-5
mounting 3-6 to 3-8
placement F-2
rotating 3-8
specifications A-6
antenna base, mounting 3-6 to 3-8
AP detailed information parameters (site survey utility) F-12 to F-13
AP Detailed Information window (site survey utility) F-12
AP scan list
parameters F-10 to F-11
pausing F-11
viewing F-9 to F-11
AP Scan List tab (site survey utility), using F-8 to F-14
AP scan log file, generating in site survey utility F-14

associated AP status parameters (site survey utility) F-6 to F-8
Associated AP Status tab (site survey utility)
units as a percentage F-5
units in dBm F-5
using F-4 to F-8
association
rejections 7-15
time-outs 7-15
ASTU
See Aironet System Tray Utility (ASTU)
ATIM Window, in site survey utility F-13
audience of document xii
authentication
process 5-17, E-4
rejections 7-15
time-outs 7-15
type
setting 5-12
status of 7-8
Authentication Timeout Value parameter
for EAP-FAST 5-33
for LEAP 5-29
Automatically Prompt for User Name and Password option
for EAP-FAST 5-33
for LEAP 5-29
auto profile selection
enabling 4-9
including a profile in 4-7 to 4-8
prioritizing profiles 4-8
removing a profile from 4-8
restrictions 4-8
status of 8-10
using 8-8
Auto Profile Selection Management window 4-7
Auto Select Profiles parameter 4-9
Available Infrastructure and Ad Hoc Networks window 4-4

B

beacon period, in site survey utility F-13
beacons received
in ADU 7-14
in site survey utility F-7
broadcast key rotation
described 5-20
setting on client and access point 5-24
broadcast packets
number received 7-13
number transmitted 7-13
broadcast SSIDs 5-4, E-6
BSS Aging Interval parameter (Windows Control Panel) 5-56
bytes
number received 7-13
number transmitted 7-13

C

CAM
See Constantly Awake Mode (CAM)
Canadian compliance statement C-3
card name 9-9
caution, defined xiii
CCKM fast secure roaming
described 5-18 to 5-19
enabling with EAP-FAST 5-31
enabling with EAP-TLS 5-40
enabling with LEAP 5-28
enabling with PEAP (EAP-GTC) 5-42
enabling with PEAP (EAP-MSCHAP V2) 5-46
setting on client and access point 5-23
CCX, version supported by access point F-11
certificates, required for EAP-TLS and PEAP authentication 5-39

channel of access point
in ADU 4-5
in site survey utility F-6, F-10, F-13
channel of client adapter 7-6, 7-11
Channel parameter 5-11
channels, supported by regulatory domains
IEEE 802.11a D-2
IEEE 802.11b/g D-3
channel set, for which client adapter is configured 7-11
Choose Destination Location window (Install Wizard) 3-14
Cisco.com
accessing xv
obtaining documentation xv
Cisco Aironet 802.11a/b/g Wireless Adapter Properties window 5-55
Cisco Aironet Desktop Utility (Diagnostics) window 7-12
Cisco Aironet Desktop Utility (Profile Management) window 4-2
Cisco Aironet Installation Program window (Install Wizard) 3-11
Cisco Centralized Key Management (CCKM)
See CCKM fast secure roaming
Cisco Key Integrity Protocol (CKIP)
statistics 7-15
status of 7-6
with LEAP 5-15
Cisco publications xix
client adapter
association status in site survey utility F-4
selecting in site survey utility F-3 to F-4
client name 9-9
Client Name parameter 5-4
client utilities
See Aironet Desktop Utility (ADU) and Aironet System Tray Utility (ASTU)
Configuration Settings window
for PEAP (EAP-GTC) 5-44
for PEAP (EAP-MSCHAP V2) 5-47
configuring client adapter
deciding between ADU and Windows XP 3-17 to 3-18
in ADU 5-1 to 5-51
in Windows XP E-5 to E-10
connection status 8-4, 8-10
Connection Status window (ASTU) 8-9
Constantly Awake Mode (CAM) 5-8
Contents menu option, in site survey utility F-15
conventions of document xiii to xiv
CRC errors 7-14
CTS frames 7-14
Current Status window 7-4

D

Data Display parameter 7-3, 7-12
data encryption
in ADU 7-7
in site survey utility F-10, F-13
data frames 7-14
data rate
in ADU 7-5
mismatches 7-14
of access point, in site survey utility F-13
setting 5-10
specifications A-3
when performing a site survey F-2
declarations of conformity
European community, Switzerland, Norway, Iceland, and Liechtenstein C-3 to C-7
FCC C-2
RF exposure C-7
default values, using 5-2
Define Certificate window 5-40
Define PEAP (EAP-GTC) Configuration window 5-43
Define PEAP (EAP-MSCHAP V2) Configuration window 5-46
Define Pre-Shared Keys window 5-24
Define WPA/WPA2 Pre-Shared Key window 5-26

diagnosing client adapter operation 10-3 to 10-6
Diagnostics window 7-12
Disable Radio
  ADU menu option 9-10
  ASTU menu option 8-7
Display in Percent parameter (site survey utility) F-4
Display Settings
  ADU menu option 7-2
  window 7-2
display units, specifying in site survey utility F-4
diversity antenna 1-3
document
  audience xii
  conventions xiii to xiv
  organization xii to xiii
  purpose xii
documentation
  feedback xvi
  obtaining xv to xvi
  ordering xvi
domain name
  including in Windows login
    for EAP-FAST 5-33
    for LEAP 5-29
  specifying for saved user name and password
    for EAP-FAST 5-33
    for LEAP 5-29
driver
  current version 9-9
  date 9-9
  described 1-4
  name 9-9
DSConfig, in site survey utility F-13
duplicate frames, number received 7-14
dwell time, in site survey utility F-13
dynamic WEP keys, overview 5-15 to 5-17, E-3 to E-4

E

EAP authentication
  described E-4
  overview 5-15 to 5-17, 6-2, E-3 to E-4
  restarting 6-15
  using 6-1 to 6-15
EAP-Cisco Wireless
  See LEAP authentication
EAP-FAST authentication
  authenticating after a reboot/logon
    with automatically prompted login 6-6 to 6-7
    with saved username and password 6-12
    with Windows username and password 6-4
  authenticating after a reboot/logon/card insertion, with manually prompted login 6-9 to 6-11
  authenticating after EAP-FAST password expires
    with automatically prompted login 6-7 to 6-8
    with manually prompted login 6-11
    with saved username and password 6-13
    with Windows username and password 6-4 to 6-5
  authenticating after profile activation, with manually prompted login 6-8 to 6-9
  authenticating after profile activation/card insertion
    with automatically prompted login 6-5 to 6-6
    with saved username and password 6-12
    with Windows username and password 6-3 to 6-4
  described 5-15 to 5-17
  disabling 5-51
  enabling 5-31 to 5-38
  overview 6-2 to 6-3
  RADIUS servers supported 5-15
  requirements 5-31
  setting on client and access point 5-21
  stages of 6-3
  user databases supported 5-16
EAP-FAST Authentication Status window
  displayed 6-2
  minimizing 6-3

EAP-FAST option 5-31
EAP-FAST Settings window 5-32
EAP MSCHAPv2 Properties window - Windows XP E-15
EAP-TLS authentication
  authenticating after profile activation/card insertion/reboot/logon 6-13
  described 5-16 to 5-17, E-3, E-4
  disabling 5-51
  enabling
    in ADU 5-39 to 5-42
    in Windows XP E-10 to E-12
  RADIUS servers supported 5-16, E-3
  requirements 5-39
  setting on client and access point 5-22
EAP-TLS machine authentication with machine credentials
  requirements 5-39
  setting 5-41
EAP-TLS option 5-40
EIRP, maximum supported by regulatory domains
  IEEE 802.11a D-4
  IEEE 802.11b D-4
  IEEE 802.11g D-5
Enable Radio
  ADU menu option 9-10
  ASTU menu option 8-7
Enable Tray Icon, ADU menu option 8-6
encryption errors 7-14
Enter Password window 5-36
Enter Wireless Network Password window 6-6, 6-7, 6-9, 6-10
error messages 10-12 to 10-22
errors
  CRC 7-14
  encryption 7-14
  MIC 7-15
Exit menu option
  in ADU 9-7
  in ASTU 8-6, 9-7
  in site survey utility F-15
Export button 4-11
Export Profile window 4-12

F

Fast PSP 5-8
FCC
  declaration of conformity statement C-2
  safety compliance statement 2-2
frames
  ACK 7-14
  CTS 7-14
  duplicate 7-14
  number dropped 7-14
  number received successfully 7-14
  number received with errors 7-14
  number retried 7-14
  number transmitted successfully 7-14
  RTS 7-14
frequencies, supported by regulatory domains
  IEEE 802.11a D-2
  IEEE 802.11b/g D-3
frequency
  in ADU 7-5, 7-11
  of access point, in site survey utility F-10, F-13
  setting 5-10

G

general parameters
  described 5-2
  setting 5-3 to 5-5
Generic Token Card Properties window - Windows XP E-17
global PACs 5-16, 5-35
Group Policy, described 3-20
Group Policy Delay parameter
  installing hot fix for 3-20 to 3-21
  setting with EAP-FAST 5-38

setting with EAP-TLS 5-42
setting with LEAP 5-30
setting with PEAP (EAP-GTC) 5-45
setting with PEAP (EAP-MSCHAP V2) 5-48
setting with PEAP (EAP-MSCHAP V2) machine authentication with machine credentials 5-49
setting with WPA/WPA2 passphrase 5-27

H

hardware components of client adapter 1-3
help
in ADU 9-9
in ASTU 8-5
in site survey utility F-15
hop pattern, in site survey utility F-13
hop set, in site survey utility F-13
Host Based EAP option 5-49
host devices 2-4

I

I/O range 10-9
Import button 4-11
Import EAP-FAST PAC File window 5-35
Import Profile window 4-11
Include Windows Logon Domain with User Name parameter
for EAP-FAST 5-33
for LEAP 5-29
information about client adapter 9-8 to 9-9
infrastructure device, defined 1-2
infrastructure mode, in site survey utility F-13
infrastructure network
selecting in ADU 5-9
wireless LAN configuration 1-6
inserting client adapter 3-2 to 3-8
Install Cisco Aironet Site Survey Utility window (Install Wizard) 3-13
installing client adapter software 3-9 to 3-20
Install Wizard file
described 1-4
installing 3-9 to 3-20
name 3-9
removing 9-6
interference 2-5, 3-6
interrupt request (IRQ) 10-9
introduction to client adapters 1-2
IP address
of access point
in ADU 7-9
in ASTU 8-11
in site survey utility F-6
of client adapter 7-6, 8-5, 8-11

J

Japan, guidelines for operating client adapters C-7

K

key icon 4-5

L

LEAP authentication
authenticating after a reboot/logon
with automatically prompted login 6-6 to 6-7
with saved username and password 6-12
with Windows username and password 6-4
authenticating after a reboot/logon/card insertion, with manually prompted login 6-9 to 6-11
authenticating after profile activation, with manually prompted login 6-8 to 6-9
authenticating after profile activation/card insertion
with automatically prompted login 6-5 to 6-6
with saved username and password 6-12
with Windows username and password 6-3 to 6-4

described 5-15 to 5-17
disabling 5-51
enabling 5-27 to 5-30
overview 6-2 to 6-3
RADIUS servers supported 5-15
requirements 5-27
setting on client and access point 5-21
stages of 6-3
timeout value 4-9, 8-8
using with login scripts 4-9
LEAP Authentication Status window
displayed 6-2
minimizing 6-3
LEAP option 5-28
LEAP Settings window 5-28
LEDs
described 1-3
interpreting 10-2
link quality
in ASTU 8-5, 8-11
in site survey utility F-8
link speed
in ASTU 8-5
in site survey utility F-8
List Installed Devices Even If Not Present in System parameter (site survey utility) F-4
log file, generating in site survey utility F-14
login scripts, using with LEAP 4-9, 8-9
Log Snapshot button, in site survey utility F-14
long radio headers
status of 7-11
using 5-9

M

MAC address
of access point
in site survey utility F-6, F-10, F-12
specifying 5-13
viewing 7-9
of client adapter 9-9
machine authentication with machine credentials
using EAP-TLS 5-41
using PEAP (EAP-MSCHAP V2) 5-49 to 5-50
machine authentication with user credentials
using PEAP (EAP-GTC) 5-43
using PEAP (EAP-MSCHAP V2) 5-47
Manual Login
ADU menu option 5-29, 6-9
ASTU menu option 8-8
Manually Prompt for User Name and Password option
for EAP-FAST 5-33
for LEAP 5-29
Max PSP 5-8
message integrity check (MIC)
described 5-20, 7-8
errors 7-15
setting on client and access point 5-23
statistics 7-15
status of 7-8
types of 7-8
with WPA 5-18
Michael MIC, status of 7-8
microcellular network 1-6
Microsoft 802.1X supplicant, disabling 10-8
Microsoft hot fix
installing 3-20 to 3-21
required for Group Policy Delay parameter 3-20
Microsoft Wireless Configuration Manager
disabling 10-8
enabling in Install Wizard 3-17
role in switching between host-based EAP and non-host-based EAP profiles 5-49, 5-50
MMH MIC
status of 7-8
with LEAP 5-15
Modify button 4-10, 5-3

multicast packets
number received 7-13
number transmitted 7-13

N

network
configurations 1-5 to 1-6
prioritizing connections 10-11
problems connecting to 10-11
type, current 4-3, 7-5
network name
in ADU 5-4, 7-7
in ASTU 8-3
in site survey utility F-10, F-12
Network Type parameter 5-9
New button 4-4, 5-3
noise level
in ADU 7-10
in site survey utility F-7
No Network Connection Unless User Is Logged In parameter
for EAP-FAST 5-33, 6-12
for LEAP 5-29, 6-12
note, defined xiii

O

online help
for ADU 9-9
for ASTU 8-5
for site survey utility F-15
Open Aironet Desktop Utility, ASTU menu option 8-6, 9-7
open authentication
setting 5-12, E-8
status of 7-8
operating systems supported xii, 2-4, 3-9
Order Profiles button 4-7
organization of document xii to xiii

P

PAC authority, selecting 5-34, 5-37
package contents 2-3
packets
broadcast 7-13
multicast 7-13
unicast 7-13
PAC provisioning
automatic 5-33 to 5-34
manual 5-33 to 5-34
PACs
copying from private store to global store 5-37
deleting 5-38
described 5-15, 5-16, 5-33
entering password for 5-36 to 5-37
importing 5-34 to 5-37
rules for storage 5-16
types of 5-16
PAC stores
selecting 5-35
types of 5-35
Pause List Update button, in site survey utility F-11
PC-Cardbus card
antenna 1-3
described 1-2
inserting 3-2
profiles tied to slot 4-6
removing 9-2
PCI card
antenna
assembling 3-5 to 3-6
described 1-3
mounting 3-6 to 3-8
rotating 3-8
changing bracket 3-3
described 1-2
inserting 3-3 to 3-8
removing 9-2

PEAP (EAP-GTC) authentication
authenticating after profile activation/card insertion/reboot/logon 6-14
described 5-17, E-3, E-4
disabling 5-51
enabling
in ADU 5-42 to 5-45
in Windows XP E-13 to E-14, E-16 to E-18
RADIUS servers supported 5-17, E-3
requirements 5-39
setting on client and access point 5-22 to 5-23
user databases supported 5-17
PEAP (EAP-GTC) machine authentication with user credentials, setting 5-43
PEAP (EAP-GTC) option 5-42
PEAP (EAP-MSCHAP V2) authentication
authenticating after profile activation/card insertion/reboot/logon 6-15
described 5-17, E-3, E-4
disabling 5-51
enabling
in ADU 5-46 to 5-48
in Windows XP E-13 to E-15
RADIUS servers supported 5-17, E-3
requirements 5-39
setting on client and access point 5-22 to 5-23
PEAP (EAP-MSCHAP V2) machine authentication with machine credentials, setting 5-49 to 5-50
PEAP (EAP-MSCHAP V2) machine authentication with user credentials, setting 5-47
PEAP (EAP-MSCHAP V2) option 5-46
PEAP Properties window - Windows XP E-16
peer-to-peer network 1-5, 5-9
physical specifications A-2
Please Change Password window 6-5, 6-8, 6-11, 6-13
power level, current 7-10
power levels, available 7-10
power save mode, currently being used 7-10
Power Save Mode parameter 5-8
power specifications A-6
Preferences, ASTU menu option 8-6
Preferred Access Points window 5-13
Preparing Setup window (Install Wizard) 3-10, 9-3
Pre-Shared Key (Static WEP) option 5-24
Previous Installation Detected window (Install Wizard) 9-4
private PACs 5-16, 5-35
product model numbers 1-2
product security
overview xvi to xvii
reporting problems xvii
profile
active 4-9, 8-3, 8-10
default 4-2
described 4-2
Profile Management (Advanced) window 5-6
Profile Management (General) window 4-6
Profile Management (Security) window 5-14
Profile Management window 4-2
Profile Management windows, parameters missing 10-11
profile manager
auto profile selection feature 4-7 to 4-8
creating a new profile 4-4 to 4-6
deleting a profile 4-10
editing a profile 4-10
exporting a profile 4-11 to 4-12
importing a profile 4-11
opening 4-2 to 4-3
parameters missing 4-3, 10-11
selecting the active profile 4-9
Profile Name parameter 5-4
profiles, losing 9-6
profiles submenu (ASTU) 8-8
Protected EAP
See PEAP (EAP-GTC) authentication and PEAP (EAP-MSCHAP V2) authentication
Protected EAP Properties window - Windows XP E-14
purpose of document xii

Q

QoS
  See quality of service
QoS Packet Scheduler
  enabling on Windows 2000 5-51 to 5-53
  enabling on Windows XP 5-54
quality of service (QoS)
  described 5-51
  in site survey utility F-11
  status of 7-9

R

radio
  described 1-3
  enabling or disabling 8-7, 9-9 to 9-10
  specifications A-2 to A-6
radio band of access point, in site survey utility F-10, F-13
RADIUS servers
  additional information 5-17, E-4
  defined 5-15, E-3
  supported 5-15 to 5-17, E-3
range 5-7
Reauthenticate menu option
  in ADU 6-15
  in ASTU 6-15, 8-8
receive rate 7-11, 8-11
receive statistics 7-13, 7-14 to 7-15
Refresh button 4-4
Refresh Interval parameter 7-3, 7-12
regulatory
  domains
    IEEE 802.11a D-2
    IEEE 802.11b/g D-3
  information C-2 to C-9
  specifications A-6
related publications xv
Remove button 4-10
removing client adapter 9-2
resource conflicts, resolving
  in Windows 2000 10-9
  in Windows XP 10-10
RF obstructions 2-5, 3-6, F-2
RM-Normal, in site survey utility F-11
RM-Source, in site survey utility F-11
roaming 1-6
roaming parameters, setting in the Windows Control Panel 5-55 to 5-56
roaming threshold 5-56
RSSI, in site survey utility F-10, F-13
RTS frames 7-14
Run Test button, in site survey utility 10-4

S

safety
  information 2-2 to 2-3
  specifications A-6
saved username and password
  described
    for EAP-FAST 5-32
    for LEAP 5-29
  entering
    for EAP-FAST 5-33
    for LEAP 5-29
Save Report
  button 10-7
  window 10-7
Scan button 4-4
Scan Valid Interval parameter (Windows Control Panel) 5-56
seamless roaming 1-6
security features
  overview 5-14 to 5-20
  synchronizing 5-20 to 5-24
security mode 4-3

security parameters
described 5-2
setting 5-13 to 5-48
Select Adapter
site survey utility menu option F-3
window (site survey utility) F-3
Select EAP-FAST PAC window 5-34
Select Network Component Type window 5-53
Select Network Service window 5-53
Select Profile, ASTU menu option 8-8 to 8-9
sensitivity A-4
serial number of client adapter 9-9
server-based authentication, currently being used 7-7
service request
definitions of severity xviii
submitting xviii
Setup Status window (Install Wizard) 9-5
Setup Type window (Install Wizard) 3-12
shared authentication
setting 5-12, E-8
status of 7-8
short radio headers
status of 7-11
using 5-9
Show Connection Status, ASTU menu option 8-9
signal quality
in ADU 7-10
in site survey utility F-7
signal strength
as a percentage 7-3
in ADU 7-6, 7-10
in ASTU 8-5
in dBm 7-3
Signal Strength Display Units parameter 7-3
signal-to-noise ratio (SNR)
as a percentage 7-3
in ADU 4-5
in dB 7-3
in site survey utility F-8
site requirements
for client devices 2-5
for infrastructure devices 2-5
site survey
environmental considerations F-2
guidelines F-2
performing F-1 to F-15
site survey utility
About window F-15
accessing help F-15
AP detailed information parameters F-12 to F-13
AP Detailed Information window F-12
AP scan list
parameters F-10 to F-11
pausing F-11
viewing F-9 to F-11
associated AP status parameters F-6 to F-8
client adapter association status F-4
exiting F-15
finding version of F-15
generating AP scan log file F-14
log file F-14
Log Snapshot button F-14
opening F-3
overview F-2
Pause List Update button F-11
selecting client adapter F-3 to F-4
specifying directory 3-13
specifying display units F-4
top of main window F-4
trend graph, explained F-6
uninstalling F-15
using AP Scan List tab F-8 to F-14
using Associated AP Status tab F-4 to F-8
View AP Details button F-12
viewing access point details F-12 to F-13
viewing status of access point F-5 to F-8
Smart Card or other Certificate Properties window - Windows XP E-11

software
compatibility with Cisco Aironet client adapters 3-9
installing 3-9 to 3-20
procedures 9-3 to 9-9
uninstalling 9-6
upgrading 9-3 to 9-5
software components of client adapter 1-4
specifications
physical A-2
power A-6
radio A-2 to A-6
regulatory compliance A-6
safety A-6
spread spectrum 1-3
SSID
setting 5-4
viewing
in ADU 4-3, 4-5, 7-7
in ASTU 8-3, 8-11
in site survey utility F-10, F-12
SSID1 parameter 5-4
SSID2 parameter 5-5
SSID3 parameter 5-5
Ssidl, in site survey utility F-11
Start Test button, in troubleshooting utility 10-5
static WEP
disabling 5-51
enabling 5-24 to 5-26
with open authentication, setting on client and access point 5-20
with shared key authentication, setting on client and access point 5-20
static WEP keys
guidelines for entering
in ADU 5-25
in Windows XP E-9
overview 5-15, E-2
selecting transmit key 5-25
size of 5-25
statistics
method of calculation 7-12
receive 7-13, 7-14 to 7-15
transmit 7-13, 7-14
viewing 7-12 to 7-15
status of client adapter
in ADU Advanced Status window 7-7 to 7-11
in ADU Current Status window 7-4 to 7-6
in ASTU Connection Status window 8-9 to 8-11
in ASTU Tool Tip window 8-4
in Windows XP E-18
Stop Test button, in troubleshooting utility 10-5
system requirements 2-4

T

Taiwan, administrative rules for client adapters C-8 to C-9
technical assistance, obtaining xvii to xviii
technical support website xvii to xviii
Temporal Key Integrity Protocol (TKIP)
described 5-20
setting on client and access point 5-24
with WPA 5-18
temporary username and password
automatically prompt for
for EAP-FAST 5-33
for LEAP 5-29
described
for EAP-FAST 5-32
for LEAP 5-29
manually prompt for
for EAP-FAST 5-33
for LEAP 5-29
selecting options
for EAP-FAST 5-33
for LEAP 5-29
using Windows credentials
for EAP-FAST 5-33
for LEAP 5-29

third-party tool, enabling in Install Wizard 3-17
throughput 5-8, 5-9
TKIP
  option in Windows XP E-8
  status of 7-6
Token Configuration window 6-14
translated safety warnings B-1 to B-6
transmit key 5-25
transmit power, in site survey utility F-11
Transmit Power Level parameter 5-7
transmit rate 7-11, 8-11
transmit statistics 7-13, 7-14
Troubleshooting
  ADU menu option 10-3
  ASTU menu option 8-6, 10-3
  button 10-3
troubleshooting information, accessing 10-2
troubleshooting utility
  saving detailed report to text file 10-7
  using 10-3 to 10-7
Troubleshooting Utility window
  detailed report 10-6
  initial window 10-4
  with test results 10-5

U

unicast packets
  number received 7-13
  number transmitted 7-13
uninstalling client adapter software 9-6
unpacking the client adapter 2-3
Unplug or Eject Hardware icon (Windows) 9-2
upgrading client adapter software 9-3 to 9-5
up time, status of 7-10
Use Auto Profile Selection, ASTU menu option 8-8
Use Machine Information For Domain Logon parameter
  for EAP-TLS 5-41
  for PEAP (EAP-GTC) 5-43
  for PEAP (EAP-MSCHAP V2) 5-47
Use Saved User Name and Password option
  for EAP-FAST 5-32
  for LEAP 5-29
Use Temporary User Name and Password option
  for EAP-FAST 5-32
  for LEAP 5-29
Use Windows to Configure My Wireless Network Settings parameter - Windows XP E-6
Use Windows User Name and Password option
  for EAP-FAST 5-33
  for LEAP 5-29

V

View AP Details button, in site survey utility F-12
View Report button 10-5

W

warning
  antenna 2-2, B-3
  defined xiii to xiv
  explosive device proximity 2-2, B-2
  laptop users 2-3, B-4 to B-6
WEP
  keys
    additional security features 5-20
    defined 5-14, E-2
    entry method 5-25
    size of 5-14, E-2
    types of 5-14, E-2
  status of 7-6
WEP key hashing, described 5-20
WEP option, in Windows XP E-8

Wi-Fi Multimedia (WMM)
enabling 5-51 to 5-54
status of 7-9
Wi-Fi Protected Access (WPA)
described 5-18, E-4
enabling in Windows XP E-8
enabling with EAP-FAST 5-31
enabling with EAP-TLS 5-40
enabling with LEAP 5-28
enabling with PEAP (EAP-GTC) 5-42
enabling with PEAP (EAP-MSCHAP V2) 5-46
software required E-4
Wi-Fi Protected Access 2 (WPA2)
described 5-18
enabling with EAP-FAST 5-31
enabling with EAP-TLS 5-40
enabling with LEAP 5-28
enabling with PEAP (EAP-GTC) 5-42
enabling with PEAP (EAP-MSCHAP V2) 5-46
Windows 2000
disabling Microsoft 802.1X supplicant 10-8
resolving resource conflicts 10-9
Windows Wireless Network Connection icon, shows unavailable connection 10-11
Windows XP
associating to an access point E-18
configuring client adapter through E-5 to E-10
disabling Microsoft Wireless Configuration Manager 10-8
enabling EAP-TLS authentication E-10 to E-12
enabling PEAP authentication E-13 to E-18
feature comparison to ADU 3-17 to 3-18
making a configuration decision 3-17 to 3-18
resolving resource conflicts 10-10
security features E-2 to E-4
viewing status of client adapter E-18
Wireless Cisco Connection Properties window 5-52
wireless infrastructure 1-6
wireless mode, current 4-5, 7-5
Wireless Mode parameter 5-10
Wireless Mode When Starting Ad Hoc Network parameter 5-10
Wireless Network Connection Properties window (Wireless Networks Tab) - Windows XP E-6
Wireless Network Connection Properties window - Windows XP 5-54
Wireless Network Connection Status window - Windows XP E-18
Wireless Network Properties window (Association Tab) - Windows XP E-7
Wireless Network Properties window (Authentication Tab) - Windows XP E-10, E-13
WMM
See Wi-Fi Multimedia
workstation
defined 1-2
in wireless infrastructure 1-6
WPA
See Wi-Fi Protected Access (WPA)
WPA/WPA2/CCKM EAP Type parameter
with EAP-FAST 5-31
with EAP-TLS 5-40
with LEAP 5-28
with PEAP (EAP-GTC) 5-42
with PEAP (EAP-MSCHAP V2) 5-46
WPA/WPA2/CCKM option
used to enable CCKM fast secure roaming 5-19
with EAP-FAST 5-31
with EAP-TLS 5-40
with LEAP 5-28
with PEAP (EAP-GTC) 5-42
with PEAP (EAP-MSCHAP V2) 5-46
WPA/WPA2 Passphrase option 5-26
WPA2
See Wi-Fi Protected Access 2 (WPA2)
WPA2 passphrase
described 5-18
disabling 5-51

enabling 5-26 to 5-27
setting on client and access point 5-21
WPA option, in Windows XP E-8
WPA passphrase
described 5-18, E-4
disabling 5-51
enabling 5-26 to 5-27
setting on client and access point 5-21
WPA Pre-Shared Key
See WPA passphrase or WPA2 passphrase
WPA-PSK
described 5-18, E-4
option in Windows XP E-8